PAESSLER
the network monitoring company

PRTG Network Monitor V8
User Manual

Bandwidth monitoring | Availability monitoring | Usage monitoring

PRTG Network Monitor 8 User Manual

© 2011 Paessler AG

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: Mai 2011 in Nuremberg

Table of Contents

Part I Welcome to PRTG Network Monitor 10

1 About this Document ... 11
2 Key Features ... 12
3 New in Version 8 ... 13
4 Available Licenses ... 16
5 System Requirements ... 18
Detailed System Requirements ... 20

Part II Quick Start Guide 26

1 ONE—Download and Installation ... 27
2 TWO—Start-Up ... 30
3 THREE—Auto-Discover Your Network ... 32

Part III Installing the Software 36

1 Download PRTG ... 37
2 Upgrade From Previous Versions to V8 ... 39
3 Install a PRTG Core Server ... 41
Setup Wizard ... 42
Welcome Wizard ... 45
4 Install a PRTG Cluster ... 53
5 Enter a License Key ... 55
6 Activate the Product ... 57
7 Install a PRTG Remote Probe ... 59
8 Install the Windows GUI ... 64
9 Uninstall PRTG Products ... 69

Part IV Understanding Basic Concepts 74

1 Architecture ... 75
2 Clustering ... 78
3 Object Hierarchy ... 79
4 Inheritance of Settings ... 82
5 Tags ... 84
6 Dependencies ... 85
7 Scheduling ... 86
8 Notifying ... 87
9 Data Reporting ... 88

© 2011 Paessler AG

10 User Access Rights 89

Part V Ajax Web Interface—Basic Procedures 92

1 Login 93
2 General Layout 97
3 Sensor States 102
4 Review Monitoring Data 104
5 Historic Data Reports 107
6 Object Settings 111
7 Alarms 113
8 Logs 115
9 ToDos 117
10 Working with Table Lists 119
11 Object Selector 120
12 Priority and Favorites 122
13 Pause 123
14 Context Menus 124
15 Hover Popup 132
16 Main Menu Structure 133

Part VI Ajax Web Interface—Device and Sensor Setup 144

1 Auto-Discovery 145
2 Create Objects Manually 156
Add a Group 157
Add a Device 160
Add a Sensor 165
3 Root Group Settings 166
4 Probe Settings 173
5 Group Settings 181
6 Device Settings 193
7 Sensor Settings 202
List of Available Sensor Types 203
Active Directory Replication Errors Sensor 210
ADO SQL Sensor 215
Amazon CloudWatch Sensor 221
Cisco IP SLA Sensor 226
Cluster Probe Health Sensor 230
Core/Probe Health Sensor 233
DHCP Sensor 236
DNS Sensor 241
Event Log (Windows API) Sensor 246
EXE/Script Sensor 251
EXE/Script Advanced Sensor 258
File Sensor 264
Folder Sensor 269

© 2011 Paessler AG

FTP Sensor ... 275
FTP Server File Count Sensor ... 280
HDD Health Sensor ... 285
HTTP Sensor ... 290
HTTP Advanced Sensor ... 295
HTTP Content Sensor ... 301
HTTP Full Web Page Sensor ... 308
HTTP SSL Certificate Expiry Sensor ... 312
HTTP Transaction Sensor ... 317
HTTP XML/REST Value Sensor ... 323
Hyper-V Host Server Sensor ... 329
Hyper-V Virtual Machine Sensor ... 333
Hyper-V Virtual Storage Device Sensor ... 337
IMAP Sensor ... 341
INI File Content Check Sensor ... 346
IP on DNS Blacklist Sensor ... 352
jFlow V5 Sensor ... 357
jFlow V5 (Custom) Sensor ... 363
LDAP Sensor ... 369
Logfile Content Check Sensor ... 374
Microsoft SQL Sensor ... 380
MySQL Sensor ... 387
NetFlow V5 Sensor ... 394
NetFlow V5 (Custom) Sensor ... 400
NetFlow V9 Sensor ... 406
NetFlow V9 (Custom) Sensor ... 412
NTP Sensor ... 418
Oracle SQL Sensor ... 423
Pingdom Sensor ... 429
Packet Sniffer (Content) Sensor ... 434
Packet Sniffer (Custom) Sensor ... 440
Packet Sniffer (Header) Sensor ... 446
Ping Sensor ... 452
Ping Jitter Sensor ... 456
Ping with Delayed Up Sensor ... 461
POP3 Sensor ... 466
POP3 Email Count Sensor ... 471
Port Sensor ... 476
QoS (Quality of Service) Sensor ... 481
RADIUS Sensor ... 487
RDP (Remote Desktop) Sensor ... 492
Sensor Factory Sensor ... 497
sFlow Sensor ... 504
sFlow (Custom) Sensor ... 510
Share Disk Free Sensor ... 516
SMTP Sensor ... 521
SMTP&IMAP Round Trip Sensor ... 527
SMTP&POP3 Round Trip Sensor ... 534
SNMP Custom Sensor ... 540
SNMP Custom String Sensor ... 546
SNMP Library Sensor ... 551
SNMP Linux Disk Free Sensor ... 558
SNMP Linux Load Average Sensor ... 563
SNMP Linux Meminfo Sensor ... 568

© 2011 Paessler AG

SNMP Traffic Sensor ... 573
SNMP Trap Receiver Sensor ... 579
SNMP Uptime Sensor ... 585
SSH Disk Free Sensor ... 589
SSH INodes Free Sensor ... 594
SSH Load Average Sensor ... 599
SSH Meminfo Sensor ... 604
SSH VMWare ESX(i) Disk Sensor ... 609
Syslog Receiver Sensor ... 614
TFTP Sensor ... 620
Traceroute Hop Count Sensor ... 625
Virtuozzo Container Disk Sensor ... 630
Virtuozzo Container Network Sensor ... 634
VMware Host Hardware (WBEM) ... 638
VMware Host Server (SOAP) Sensor ... 642
VMware Virtual Machine (SOAP) Sensor ... 646
WBEM Custom Sensor ... 651
Windows Last Update Sensor ... 656
Windows Logged In Users Sensor ... 661
Windows MSMQ Queue Length Sensor ... 666
Windows Print Queue Sensor ... 671
WMI CPU Load Sensor ... 676
WMI Custom Sensor ... 680
WMI Event Log Sensor ... 686
WMI Exchange Server 2003 Sensor ... 693
WMI Exchange Server 2007 Sensor ... 697
WMI File Sensor ... 701
WMI Free Disk Space (Single Disk) Sensor ... 706
WMI Free Disk Space (Multi Drive) Sensor ... 711
WMI IIS 6.0 SMTP Received Sensor ... 718
WMI IIS 6.0 SMTP Sent Sensor ... 722
WMI Memory Sensor ... 726
WMI Microsoft SQL Server 2005 Sensor ... 730
WMI Microsoft SQL Server 2008 Sensor ... 735
WMI Network Card Sensor ... 740
WMI Pagefile Sensor ... 744
WMI Process Sensor ... 748
WMI Service Sensor ... 753
WMI Share Sensor ... 758
WMI Terminal Services (Windows 2008) Sensor ... 764
WMI Terminal Services (Windows XP/Vista/2003) Sensor ... 768
WMI Uptime Sensor ... 772
WMI Vital System Data Sensor ... 776
WMI Windows Version Sensor ... 781
Xen Virtual Machine Sensor ... 786

8 Additional Sensor Types (Custom Sensors) ... 790

9 Sensor Channels Settings ... 792

10 Sensor Notifications Settings ... 797

Part VII Ajax Web Interface—Advanced Procedures 806

1 Toplists ... 807

2 Arrange Objects ... 811

© 2011 Paessler AG

3 Multi-Edit Lists ... 813
4 Create Device Template ... 815
5 Clone Object ... 817
6 Compare Sensors ... 819
7 Show Dependencies ... 821
8 Geo Maps ... 823
9 Notifications ... 825
10 Reports ... 827
Reports Step By Step ... 830
View and Run Reports ... 833
Reports Settings ... 835
11 Maps ... 842
Maps Step By Step ... 845
Maps Designer ... 847
Maps Settings ... 854
12 Setup ... 857
Account Settings—My Account ... 859
Account Settings—Notifications ... 862
Account Settings—Schedules ... 868
System Administration—System and Website ... 871
System Administration—Notification Delivery ... 877
System Administration—Probes ... 881
System Administration—Cluster ... 883
System Administration—User Accounts ... 884
System Administration—User Groups ... 887
PRTG Status—System Status ... 888
Downloads ... 890

Part VIII Windows GUI 894

1 First Start ... 895
2 General Layout ... 897
3 Menu Tabs and Page Content ... 899
Devices ... 900
Sensors ... 904
Alarms ... 906
Maps ... 907
Reports ... 908
Logs ... 909
ToDos ... 911
Setup ... 912
4 Options and Server Settings ... 913
5 Windows Menu Structure ... 919
6 Context Menus ... 922
7 Shortcuts Overview ... 923

Part IX Other User Interfaces 926

1 HTML GUI (Low bandwidth) ... 927

© 2011 Paessler AG

2 Smart Phone Apps ... 930

Part X Sensor Technologies 934

1 Monitoring via SNMP ... 935
2 Monitoring via WMI ... 938
3 Monitoring Bandwidth via Packet Sniffing ... 940
4 Monitoring Bandwidth via Flows ... 942
5 Bandwidth Monitoring Comparison ... 944
6 Monitoring Quality of Service ... 947
7 Monitoring Email Round Trip ... 951

Part XI System Administration Programs 954

1 PRTG Server Administrator ... 955
2 PRTG Probe Administrator ... 969

Part XII Advanced Topics 978

1 Application Programming Interface (API) Definition ... 979
2 Filter Rules for xFlow and Packet Sniffer Sensors ... 980
3 Channel Definitions for xFlow and Packet Sniffer Sensors ... 982
4 Define IP Ranges ... 984
5 Regular Expressions ... 985
6 Add Remote Probe ... 986
Remote Probes and Multiple Probes ... 987
Remote Probe Setup ... 990
7 Calculating Percentiles ... 995

Part XIII Appendix 998

1 Glossary ... 999
2 List of Abbreviations ... 1002
3 Support and Troubleshooting ... 1004
4 Legal Notices ... 1005

Index 1007

© 2011 Paessler AG

Part I

Welcome to PRTG Network Monitor

1 Welcome to PRTG Network Monitor

Welcome to PRTG Network Monitor! You've chosen an easy-to-use software product that comes with a powerful set of features to monitor your entire network.

Why Network Monitoring is Important

Today, most businesses rely on a computer and network infrastructure for Internet, internal management, telephone and email. A complex set of servers and network equipment is required to ensure that business data flows seamlessly between employees, offices, and customers. The economical success of an organization is tightly connected with the flow of data.

The computer network's reliability, speed, and efficiency are crucial for businesses to be successful. But, like all other technical objects, network devices may fail from time to time—potentially causing trouble and loss of sales, no matter what migration efforts have been made up-front.

Network administrators need to take three key steps to maintain network uptime, reliability and speed:

1. Set up a well-planned network with reliable components.
2. Create recovery plans for the event of device failure.
3. Monitor their network to know about failures as they build up or actually happen.

PRTG Network Monitor, the software described in this document, is a complete solution for monitoring small, medium, and large networks.

Monitoring Networks with PRTG Network Monitor

PRTG Network Monitor is a powerful network monitoring application for Windows-based systems. It is suitable for small, medium, and large networks and capable of LAN, WAN, WLAN and VPN monitoring. You can also monitor real or virtual web, mail, and file servers, Linux systems, Windows clients, routers, and many more. It monitors network availability and bandwidth usage as well as various other network parameters such as quality of service, memory load and CPU usages. It provides system administrators with live readings and periodical usage trends to optimize the efficiency, layout and setup of leased lines, routers, firewalls, servers and other network components.

The software is easy to set up and use and monitors a network using Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), packet sniffer, Cisco NetFlow (and sFlow) as well as many other industry standard protocols. It runs on a Windows-based machine in your network for 24-hours every day. PRTG Network Monitor constantly records the network usage parameters and the availability of network systems. The recorded data is stored in an internal database for later analysis.

© 2011 Paessler AG

1.1 About this Document

This document introduces you to the system concepts of **PRTG Network Monitor** and explains how to set up the software to achieve the best monitoring results. You will learn how to plan your monitoring setup, how to set up your devices and sensors, dependencies, reports, notifications, maps, user accounts, and clustering for fail-safe monitoring.

This document is also meant as a reference for all available settings. Short contextual help is already provided within the Ajax web interface; in this manual you often get some more help regarding the different options available.

This document does *not* explain monitoring protocols and file formats in-depth. Also, the use of the Application Programming Interface (API) built into PRTG is only briefly addressed. Whenever possible, hyperlinks to more detailed resources are provided, such as articles in the Paessler Knowledge Base.

To start using PRTG right away, please see the Quick Start Guide 26 section. For more detailed instructions, see the other sections.

1.2 Key Features

PRTG monitors your network and requires no third party software.

What PRTG Can Be Used For

- Monitor and alert for uptimes/downtimes or slow servers.
- Monitor and account bandwidth and network device usage.
- Monitor system usage (CPU loads, free memory, free disk space etc.).
- Classify network traffic by source/destination and content.
- Discover unusual, suspicious or malicious activity with devices or users.
- Measure QoS and VoIP parameters and control service level agreements (SLA).
- Discover and assess network devices.
- Monitor fail-safe using a failover cluster setup.

What PRTG Includes

The PRTG installer contains all modules and software necessary to run the monitoring system without the need for third party modules, including:

- Paessler's own fast and efficient database system to store the raw monitoring results (outperforms SQL servers for monitoring data).
- Built-in web server with HTTP and HTTPS support for the user interface.
- Mail server for automatic email delivery.
- SQLite SQL Server for storage of events, toplists and ToDos.
- Report generator to create reports in HTML or Portable Document Format (PDF).
- Graphics engine for user-friendly charts.
- Network analysis module to auto-discover devices and sensors.
- An Application Programming Interface (API) allows users to program their own features.

PRTG Network Monitor can support thousands of sensors and can optionally work with multiple remote probes to monitor multiple sites or network segments from one central core installation.

The software is based on Paessler's reliable monitoring technology, which has been constantly improved since 1997 and is already used by more than 150,000 users around the world every day. Attractive licensing packages from freeware (up to 10 sensors) to enterprise level (with thousands of sensors) make sure that every user finds the proper solution.

© 2011 Paessler AG

1.3 New in Version 8

PRTG V8 comes with a lot of new features, making comprehensive network monitoring even easier. Changes and new features include:

- New: Clustering 13
- Improved: Web Interface 13
- Improved: Maps Feature 14
- New: Native and Agent-Less Linux Monitoring 14
- New: Plenty of New Sensor Types 14
- New: Plenty of New Features 14
- Improved: Speed and Stability 15
- Other Technical Changes 15
- Licensing Changes 15

New: Clustering

You can setup up to 5 PRTG instances working together in a cluster, enabling fail-safe monitoring

- A cluster consists of one primary instance of PRTG ("Master Node") and 1 to 4 secondary servers ("Failover Nodes")
- Objective 1: Achieve 100% uptime for the monitoring solution. Not even a software update causes downtime for a PRTG cluster.
- Objective 2: Automatic failover: If the primary node fails or loses connection to the cluster, another node immediately becomes the master server and manages notifications. Thus, notifications are always sent, even if the primary master has no connectivity or has crashed.
- Objective 3: Multiple points-of-presence monitoring: All nodes monitor all sensors all the time. This means that response times are measured from different locations in the network (LAN/WAN/VPN) and can be compared with each other. Additionally, aggregated up/downtimes can be computed.
- Reports can be generated "per node" or "for all nodes"
- And here comes the best part of this new feature—our customer-friendly licensing: All PRTG licenses allow you to create a "Single Failover" installation 53 (two installations of PRTG working together) with just one license key (additional license keys are required for 3 or more nodes).
- This means that you don't pay extra to use PRTG's new high-availability feature (compare with other vendors!). We expect that most commercial PRTG installations will be "Single-Failover" installations (1 primary node plus 1 failover node).

Improved: Web Interface

PRTG's Asynchronous Java Script and XML (AJAX) web interface 92 has been improved and redesigned.

- We've rearranged the web interface, added new on-mouse-over features and redesigned the overall look and feel to make the web interface even more convenient for your daily work. Literally hundreds of changes and optimizations are waiting to be discovered!
- Added a "Mini HTML" (HTML GUI 927) interface for mobile and low bandwidth access designed for and tested with iOS (iPhone/iPad), Android, Blackberry, Windows Mobile, Opera Mini, and even Internet Explorer 5/6/7 (the HTML GUI does not require Ajax/Javascript but has only limited functionality)
- Support for Google Maps in the web interface (maps that show red/green/etc. flags for down/up/etc. devices). Simply enter a postal address, city name, or geo tag in the "location" field of groups and/or devices to populate the maps with live monitoring data!

Improved: Maps Feature

The Maps functions have been extended.

- PRTG now includes 280 beautifully designed network icons and you can connect map 842 objects with lines that follow their objects when they are moved. With the new editor, PRTG now supports you in creating maps of your whole network structure, even without additional background graphics.

New: Native and Agent-Less Linux Monitoring

- In-depth monitoring of Linux systems using dedicated sensors 204, without extensive modifications on the clients
- Uses Secure Shell (SSH), Web-Based Enterprise Management (WBEM), or Simple Network Management Protocol (SNMP) for monitoring
- Support for all major Linux distributions and Mac OS X

New: Plenty of New Sensor Types

PRTG now offers more than 110 different sensor types. New and improved sensor types include:

- TFTP sensor 620
- NTP sensor 418
- ADO SQL sensor 215 (i.e. support for all ADO compatible databases)
- LDAP sensor 369
- XEN Virtual Machine sensor 786
- Hyper-V Virtual Storage Device sensor 337
- WMI Terminal Services sensor 768
- WMI Share sensor 758
- WMI Uptime sensor 772
- Windows Event Log sensor (Windows API based) 246
- Linux SSH sensors (Load Average 599, Meminfo 604, Disk Free 589)
- Linux SNMP sensors (Load Average 563, Meminfo 568, Disk Free 558)
- VMware Host Hardware sensor (using WBEM) 638
- WBEM Custom sensor 651
- HTTP sensors 203 now with proxy support

New: Plenty of New Features

The new and improved features introduced in version 8 include:

- New chart types: PRTG's charts are now easier to read with the optional new "filled" and "stacked" styles. For traffic sensors the in and out channel can be shown as positive and negative value.
- Improved email notifications: Notification HTML emails now look great on most email clients.
- Improved notification summarizing (to avoid email floodings)
- HTTP notifications now with proxy support
- Improved connection management for Windows Management Instrumentation (WMI)
- Improved Application Programming Interface (API). Many new features have been added to make it easier to create your own custom sensors and scripts.
- Added a graphical visualization of sensor dependencies

© 2011 Paessler AG

Improved: Speed and Stability

Features related to speed an stability include:

- Reporting is now fully decoupled from web server and user interface, so report generation no longer affects user experience. This allows us to ease the minimum interval limits for reports: reports with 1 minute interval can now be created for up to 40 days instead of one day, 1 hour reports are possible for up to one year now.
- Monitoring scheduler now distributes monitoring request evenly of time (per device) to avoid load peaks caused by monitoring requests
- Notifications can now be summarized in various ways, with different settings for each single notifications
- Performance improvements throughout the entire software

Other Technical Changes

Changes in version 8 include:

- Dropped support for Flash graphs in the web interface
- Dropped support for Internet Explorer 7 for the Ajax interface (minimum browser requirement for the Ajax interface: IE8, Firefox 3 or 4, or Chrome)
- Oracle SQL sensor now uses external process for improved stability

Licensing Changes

We've extended and simplified our license model:

- Cluster functionality included in all editions, including freeware
- One PRTG license key may now be installed on two computers in order to set up a failover cluster
- Unlimited number of xFlow (NetFlow, sFlow) sensors per PRTG installation (no more add-on licenses) in all editions, including freeware
- Unlimited number of probes per PRTG installation in all editions, including freeware

© 2011 Paessler AG

1.4 Available Licenses

There are four different PRTG flavors available.

Freeware Edition

The Freeware Edition is a good solution to get started with PRTG, or for private use:

- May be used for free for personal and commercial use.
- Can monitor up to 10 sensors.
- Supports all available sensor types.
- Shortest available monitoring interval is one minute.

Starter Edition

The Starter Edition has all the features of the Freeware Edition, but it supports up to 20 sensors. By entering a Starter Edition key, you can extend your Freeware Edition. For detailed information, see More 16 section below.

Trial Edition

The Trial Edition is intended for evaluation purposes for customers who are interested in purchasing commercial licenses:

- Can monitor up to 5,000 sensors.
- Supports all available sensor types.
- Shortest available monitoring interval is one second (a minimum interval of 10 seconds is recommended).
- Temporary license key must be requested from Paessler's website.
- Trial period limited to 30 days (automatically reverts to Freeware Edition afterwards).

As default after installation, the Trial Edition runs with the functionality of the Freeware Edition only when no license key is entered. Free trial license keys see More 16 section below.

Commercial Editions

There are several licenses of PRTG Network Monitor available to suit the demands of smaller, as well as larger customers and organizations:

- Can monitor maximum number of sensors (from 100 to unlimited).
- Supports all available sensor types.
- Shortest available monitoring interval is one second (a minimum interval of 10 seconds is recommended).

For more information about available commercial licenses, please see More 16 section below.

More

Knowledge Base: What is the PRTG Starter Edition license?

- http://www.paessler.com/knowledgebase/en/topic/8063

© 2011 Paessler AG

Paessler website: Request a Free PRTG Trial Key for Evaluation
- http://www.paessler.com/prtg/trial

Paessler FAQs: What is the difference between the PRTG Network Monitor licenses?
- http://www.paessler.com/support/faqs#e1912

1.5 System Requirements

In order to install and work with PRTG Network Monitor you need:

- A PC server or virtual machine with roughly the CPU performance of an average PC built in the year 2007 or later and minimum 1024 RAM memory. For cluster installations, use systems with similar performance.
- Operating system Microsoft Windows XP, Windows 2003, Windows 2008 R2, or Windows 7 (32-bit or 64-bit). You can also use Windows Vista or 2008 R1, but we recommend not to use these systems, as there are known performance issues related to them.
- Web browser to access the web interface (Google Chrome is recommended; Firefox 3 or 4, Safari 5, and Internet Explorer 8 were also tested).

Planning an Installation With Hundreds of Sensors or More?

As a rule of thumb an average PC/server built in the year 2007 or later should be able to monitor 1,000 sensors with ease. Some exceptions apply for version 3 of Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI) and packet sniffer. The maximum number of sensors you can monitor with one installation of PRTG mainly depends on the monitoring technology and the monitoring intervals you use:

- **SNMP V1** and **V2**, **Ping**, **Port**, and **HTTP**
  These sensor types are recommended for scenarios with thousands of sensors. With these technologies up to 30,000 sensors are possible.
- **SNMP V3**
  You will be able to monitor between 60 and 6,000 SNMP V3 sensors with an interval of 60 seconds (depending on request times in your network).
- **WMI**
  Try to keep the number of WMI sensors per probe below 120 sensors (with 60s interval), or 600 sensors (with 300s interval).
- **xFlow (NetFlow, sFlow)**
  Monitoring the maximum number of sensors depends on the traffic pattern, the number of xFlow packets per second received by the PRTG probe, as well as the performance of the probe system (see site planner tool linked in the **More** 19 section below).
- **Packet Sniffer**
  These sensors create the highest CPU load on the probe system. This technology is only recommended for monitoring of low traffic connections (<50 Mbit/s steady stream). When traffic is often over 10 Mbit/s a dedicated remote probe 986 should be used.

To overcome any limitations mentioned above you should distribute the sensors over two remote probes 986 or more. For detailed information please use the site planner tool to plan large installations. See **More** 19 section below.

© 2011 Paessler AG

For more information please see the **Detailed System Requirements** 20 section.

More

Paessler website: Paessler PRTG 7 Site Planner Tool
- http://media.paessler.com/publicimages/prtg7siteplanner.htm

Knowledge Base: How can I speed up PRTG—especially for large installations?
- http://www.paessler.com/knowledgebase/en/topic/2733

1.5.1 Detailed System Requirements

This section lists different aspects of system requirements for PRTG:

- Supported Operating Systems 20
- Hardware Requirements 20
- Sample Configurations 21
- Running PRTG on Virtual Machines 23
- Web Browser Requirements 23
- Requirements for Monitored Devices 24
- Requirements for the Windows GUI 24
- Requirements for HTML GUI 24
- Requirements for Smart Phones 24
- More 24

Supported Operating Systems

The 32-bit and 64-bit versions of the following operating systems are officially supported for PRTG **Core Service** and **Probe Service** (Intel x86/x64 architectures only):

- Microsoft Windows XP
- Microsoft Windows Server 2003
- Microsoft Windows Vista*
- Microsoft Windows Server 2008*
- Microsoft Windows Server 2008 R2
- Microsoft Windows 7

* For performance reasons, we recommend to not use Windows Vista or 2008 R1, especially when monitoring via Windows Management Instrumentation (WMI). Using these operating systems you will only be able to use a limited number of WMI sensors! For detailed information please see More 24 section below.

Hardware Requirements

Hardware requirements for PRTG **Core Service** and **Probe Service** mainly depend on the sensor types and intervals used. The following values are provided as reference for common usage scenarios of PRTG 8 (based on a default sensor interval of 60 seconds).

- **CPU**
  An average PC built in 2007 can easily monitor 1,000 sensors (see sensor type specific notes below). PRTG supports native x86 architectures.

- **RAM memory**
  Minimum requirement: 1024 MB RAM. You will need about 150 KB of RAM per sensor.

- **Hard Disk Drive**
  You will need about 200 KB of disk space per sensor per day (for sensors with 60 second interval).

© 2011 Paessler AG

- **Internet connection**
  An Internet connection is required for license activation (via HTTP or email).

There are also non-hardware dependent limitations for some sensor types, e.g. WMI and SNMP V3 sensors. These limitations can be overcome by distributing the sensors across multiple remote probes 986. If you plan installations with more than 500 to 1,000 sensors, or more than 10 Packet Sniffer or xFlow (NetFlow, sFlow) sensors, please consult the site planner tool linked in the **More** 24 section below.

Sample Configurations

The sample configurations in the table below will give you an overview of the hardware requirements for PRTG, based on your configuration.

	Large Installation A	Large Installation B	Netbook Installation
System	DELL Alienware	DELL PowerEdge 2900 III	DELL Inspiron Mini 10
CPU	Intel Core2 Quad-Core 2.6 GHz	Intel Xeon Quad-Core 1.87 GHz	Intel Atom Z520 1.33 GHz
RAM	8 GB	16 GB	1 GB
Operating System	Windows 7 64-Bit	Windows 2003 64-Bit	Windows XP 32-Bit
Sensors	20,000 SNMP 100 Other	20,000 SNMP	600 SNMP 750 WMI
Installation Corresponds To	400 switches à 48 ports	400 switches à 48 ports	24 switches à 25 ports + 30 Windows server
Scanning Interval	1 minute	1 minute	5 minutes
Number of Probes	4	1	1
Average CPU Load While Monitoring*	3 %	20 %	35 %
Average CPU Load While Generating Reports*	20 %	30 %	85 %
Average Memory Used	3 GB	3.5 GB	260 MB
Average Data Written to Disk Per Year	800 GB	800 GB	55 GB
Average Network Load	80 kbit/s	550 kbit/s	150 kbit/s

* CPU load is higher while users are accessing the web interface.

© 2011 Paessler AG

Running PRTG on Virtual Machines

PRTG core server as well as PRTG probe can be run on virtualized platforms. The following platforms were tested successfully:

VM Technology	Client OS
VMware ESX/ESXi (version 3.5 and VSphere 4)	Windows XP, Windows 2003 (32/64 bit), Windows Vista, Windows 7 (32/64 bit), Windows 2008 (32/64 bit)
VMware Server 2.0	Windows XP, Windows 2003 (32/64 bit), Windows 2008
XEN Server 5.0	Windows XP
Parallels Virtuozzo Containers	Windows 2003 Server (32/64 bit)
Cloud Hosting Platforms (Amazon EC2, TheRackspaceCloud, and others)	Windows Server 2003, Windows Server 2008

Note: When monitoring more than 1,000 sensors we recommend to use dedicated real hardware instead of a virtual machine. In our experience, this improves performance a lot.

Web Browser Requirements

The following browsers are officially supported by the PRTG web interface (in order of performance and reliability):

- Google Chrome (recommended)
- Mozilla Firefox 3 or later
- Apple Safari 5 or later
- Microsoft Internet Explorer 8 (with limited Maps functionality)

Note: Microsoft Internet Explorer version 6 and 7 are not and mobile browsers may not be able to display the full featured Ajax web interface 92. Using these browsers, you can only access the feature-limited HTML web interface 927, which does not require CSS or Javascript capability.

PRTG's web interface makes heavy use of Javascript and AJAX. We found that for some functions Chrome and Safari are up to 10 times faster than Internet Explorer 8, and 3 to 5 times faster than Firefox 3.

Internet Explorer version 8 has to be installed on the system running the PRTG core server, so PRTG's HTTP Full Web Page Sensor 308 sensor and the Windows GUI 894 can work correctly.

Requirements for Monitored Devices

- **SNMP monitoring**
  The monitored device(s) must be equipped with SNMP Version 1, 2c or 3 (i.e. a SNMP-compatible software must be installed on the device). SNMP must be enabled on the device and the machine running PRTG must be allowed access to the SNMP interface.

- **WMI monitoring**
  In order to use WMI (Windows Management Instrumentation) monitoring you will need a Windows network. For client PCs monitored with WMI only Windows XP and later are officially supported (XP, 2003, Vista, 2008, etc.). Windows 2000 is not officially supported. Please do not use Windows Vista or Windows 2008 R1 for WMI monitoring (they both have WMI performance issues).

- **xFlow (NetFlow, sFlow) monitoring**
  The device must be configured to send NetFlow data packets (NetFlow version 5 or 9) or sFlow packets (version 5) to the machine running the PRTG probe.

- **Packet Sniffer monitoring**
  Only data packets passing the local machine's network card can be analyzed. Switches with so-called 'monitoring ports' are necessary for network-wide monitoring in switched networks.

Requirements for the Windows GUI

The optional PRTG Windows GUI 894 runs under all Windows versions XP or later and requires Internet Explorer 8.

Requirements for HTML GUI

The feature-limited HTML web interface is optimized for low bandwidth and mobile access. It has been designed for and tested with iOS (iPhone, iPad), Android, Blackberry, Windows Mobile, Opera Mini, and even Internet Explorer 5/6/7.

Requirements for Smart Phones

The optional smart phone apps for iOS require firmware 3.0 (or later). For Android devices, OS 2.1 through 2.3 is recommended. For more information, please see **Smart Phone Apps** 930. The 'Mini HTML 927' interface can be used on most phones with a browser. We successfully tested it on Symbian, Blackberry, Windows, Android, and iOS devices.

More

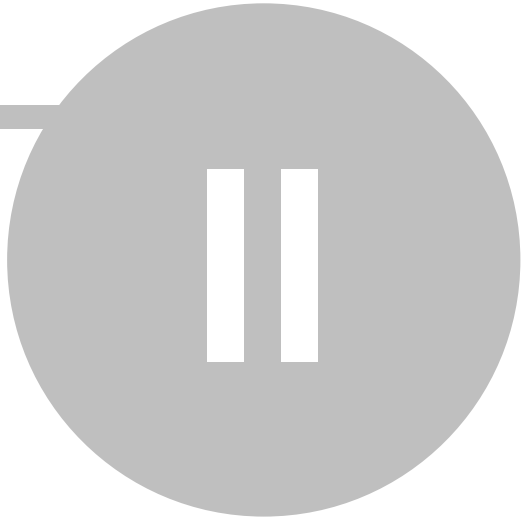
CEO's Blog: Don't Use Windows Vista And Windows 2008 R1 for Network Monitoring via WMI!
- http://www.paessler.com/blog/2010/09/22/

Paessler Website: Paessler PRTG 7 Site Planner Tool
- http://media.paessler.com/publicimages/prtg7siteplanner.htm

Knowledge Base: How can I speed up PRTG—especially for large installations?
- http://www.paessler.com/knowledgebase/en/topic/2733

© 2011 Paessler AG

Part



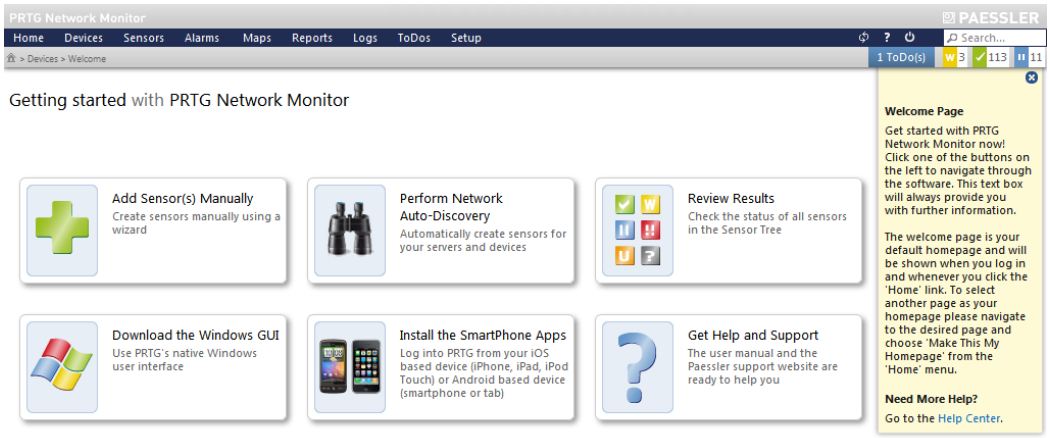
Quick Start Guide

2 Quick Start Guide

Welcome to PRTG Network Monitor! This section will support you with a quick start into PRTG, so you can start monitoring your network out-of-the box!

Setting up monitoring for your network is easy! Please see the following quick steps:

- ONE—Download and Installation 27
- TWO—Start-Up 30
- THREE—Auto-Discover Your Network 32


PRTG Network Monitor
PAESSLER
Home Devices Sensors Alarms Maps Reports Logs ToDos Setup
Search...
> Devices > Welcome
1 ToDo(s) 3 113 11
Getting started with PRTG Network Monitor
Add Sensor(s) Manually
Create sensors manually using a wizard
Perform Network Auto-Discovery
Automatically create sensors for your servers and devices
Review Results
Check the status of all sensors in the Sensor Tree
Download the Windows GUI
Use PRTG's native Windows user interface
Install the SmartPhone Apps
Log into PRTG from your iOS based device (iPhone, iPad, iPod Touch) or Android based device (smartphone or tab)
Get Help and Support
The user manual and the Paessler support website are ready to help you
Welcome Page
Get started with PRTG Network Monitor now! Click one of the buttons on the left to navigate through the software. This text box will always provide you with further information.
The welcome page is your default homepage and will be shown when you log in and whenever you click the 'Home' link. To select another page as your homepage please navigate to the desired page and choose 'Make This My Homepage' from the 'Home' menu.
Need More Help?
Go to the Help Center.

Welcome Screen

More

The quick start guide is available in different languages. Please click on the following links to open the respective PDF files.

German: Loslegen mit PRTG
- http://download.paessler.com/download/prtg8manual_gde.pdf

Spanish: Iniciar con PRTG
- http://download.paessler.com/download/prtg8manual_ges.pdf

French: Mise en route de PRTG
- http://download.paessler.com/download/prtg8manual_gfr.pdf

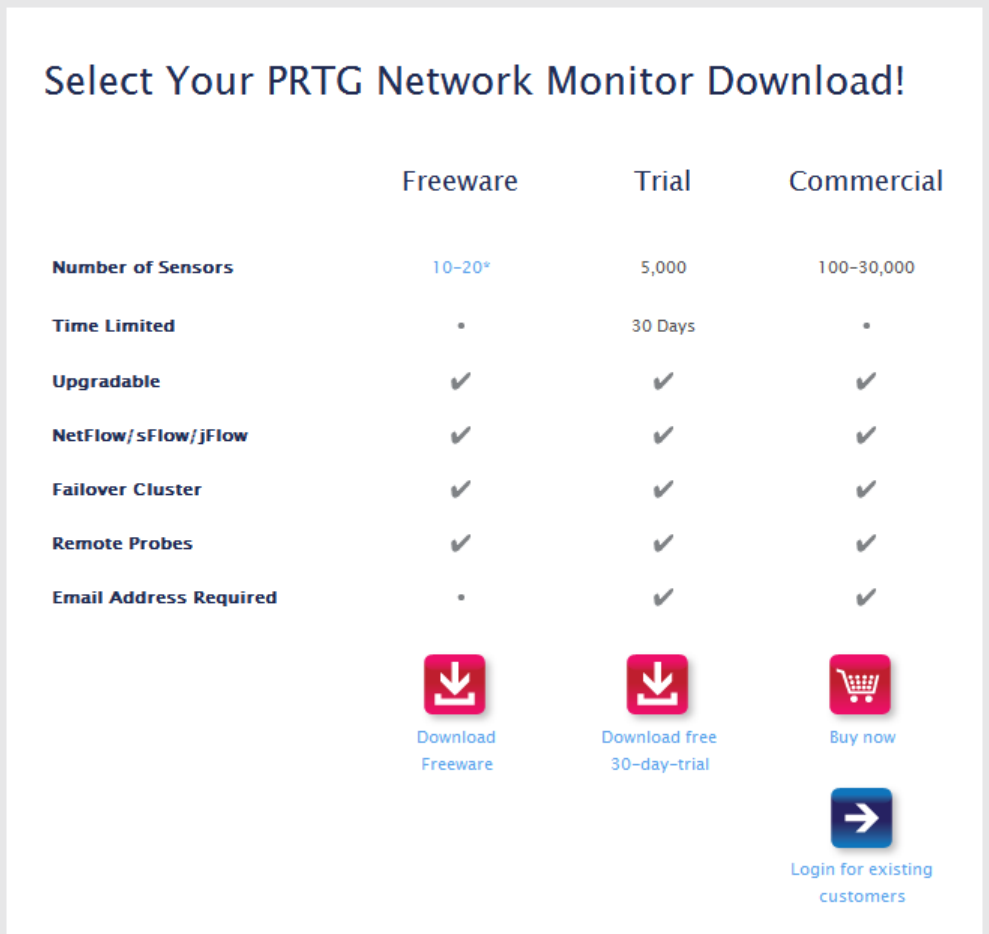
© 2011 Paessler AG

2.1 ONE—Download and Installation

Simply download and install your version of PRTG. For video instructions, please see the More 29 section below.

Download

On the Paessler website, you find two different installers for PRTG, a public download for the Freeware and Trial editions, and another download for the commercial editions (which is only available for paying customers).



PRTG Download at Paessler Website

Downloading the Freeware Edition or Trial Edition

Please download the latest publicly available file from the Paessler website. When downloading the Trial Edition, you can also request a trial key there:

- http://www.paessler.com/prtg/download

Downloading the Commercial Editions

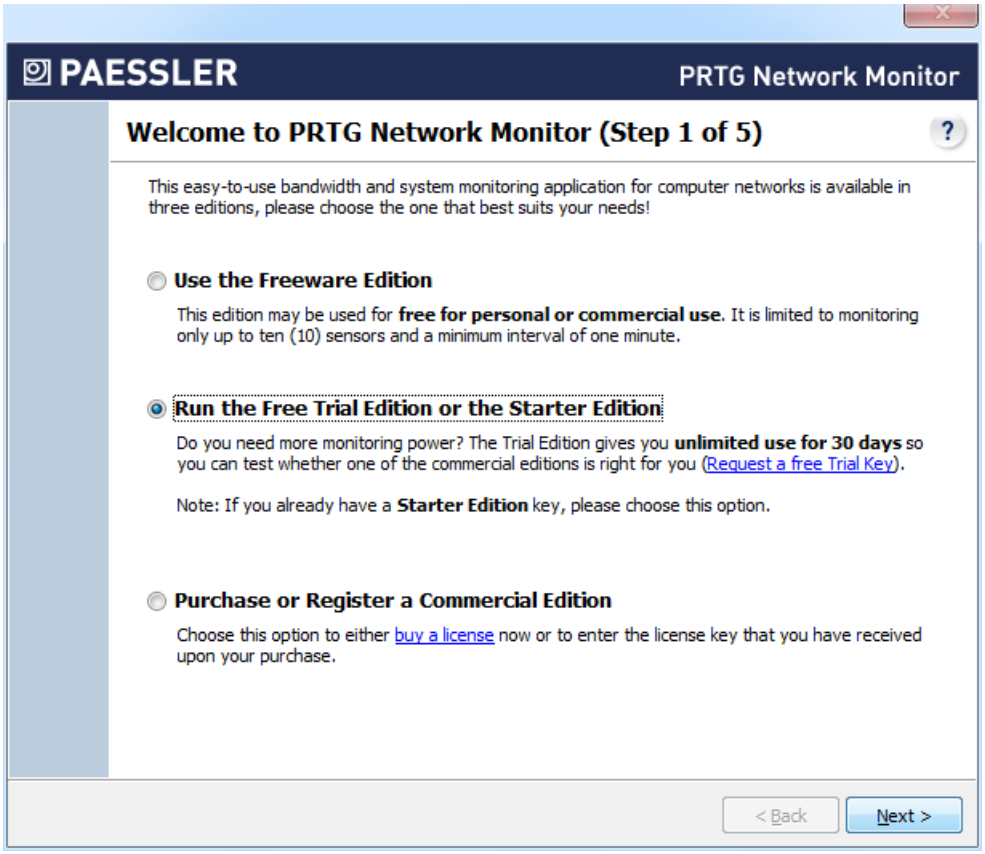
Downloads and updates are free to customers with an active maintenance contract. Please log into the Paessler website to get the latest download. You can also find your license key there:

- http://www.paessler.com/login

If you do not have an active maintenance contract, please contact sales@paessler.com.

Installation

Please double click the setup file on the computer that will be your PRTG server. Follow the installation wizard and install the software.


PAESSLER
PRTG Network Monitor
Welcome to PRTG Network Monitor (Step 1 of 5)
This easy-to-use bandwidth and system monitoring application for computer networks is available in three editions, please choose the one that best suits your needs!
Use the Freeware Edition
This edition may be used for free for personal or commercial use. It is limited to monitoring only up to ten (10) sensors and a minimum interval of one minute.
Run the Free Trial Edition or the Starter Edition
Do you need more monitoring power? The Trial Edition gives you unlimited use for 30 days so you can test whether one of the commercial editions is right for you (Request a free Trial Key).
Note: If you already have a Starter Edition key, please choose this option.
Purchase or Register a Commercial Edition
Choose this option to either buy a license now or to enter the license key that you have received upon your purchase.
< Back
Next >

Welcome Wizard

Should you have questions during the welcome wizard, please click on the blue question mark *?* symbol in the upper right corner to load a help page in your browser.

- **Step 1**: Choose the type of **Edition** you want to install.
- **Step 2**: For Trial Edition, Starter Edition, or Commercial Edition, provide your **License** information (skipped for Freeware Edition).

© 2011 Paessler AG

- **Step 3**: In the **Essential Settings**, enter a valid email address and leave the other default values.

- **Step 4**: In the **Cluster Mode Selection**, we recommend setting up your installation for **Standalone Mode**. You can extend your setup to a cluster later on.

More

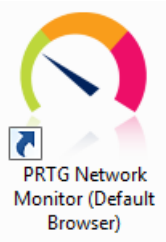
Video Tutorial: There is a video available on the Paessler video tutorials page.
- http://www.paessler.com/support/video_tutorials

2.2 TWO—Start-Up

Once installed, you can immediately log into the Ajax web interface.

Load Web Interface

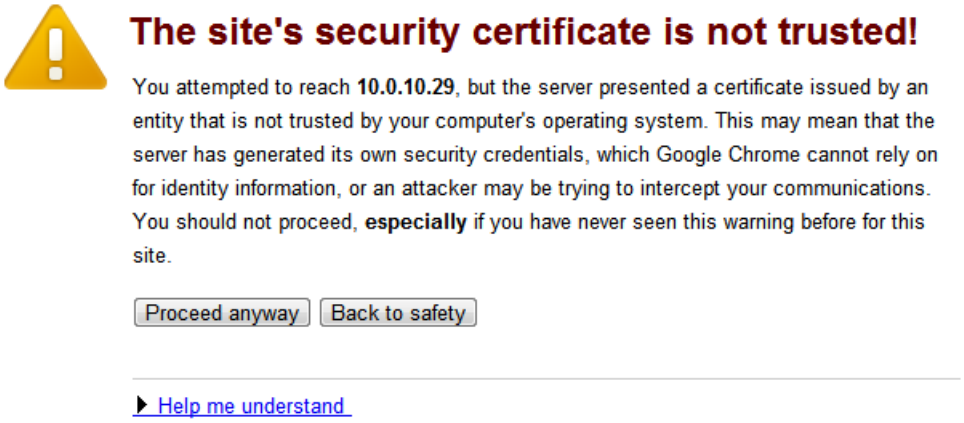
Open Google Chrome or Mozilla Firefox on the computer you've installed PRTG and enter the IP address of your own computer in the address bar. If you have set one of these browsers as standard browser, you can also double click on the **PRTG Network Monitor** icon on your desktop.



Desktop Icon

Confirm Certificate Warning

When loading the web interface, you will see a certificate warning.


The site's security certificate is not trusted!
You attempted to reach 10.0.10.29, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, especially if you have never seen this warning before for this site.
Proceed anyway
Back to safety
Help me understand

Security Warning in Google Chrome Browser

Every browser shows this warning in a different layout. The certificate that comes with PRTG is not insecure, but simply not signed by a valid authority. In order to proceed to the login screen, please confirm the claimed "security risk". The steps to take are similar for every browser, yet different in detail.

© 2011 Paessler AG

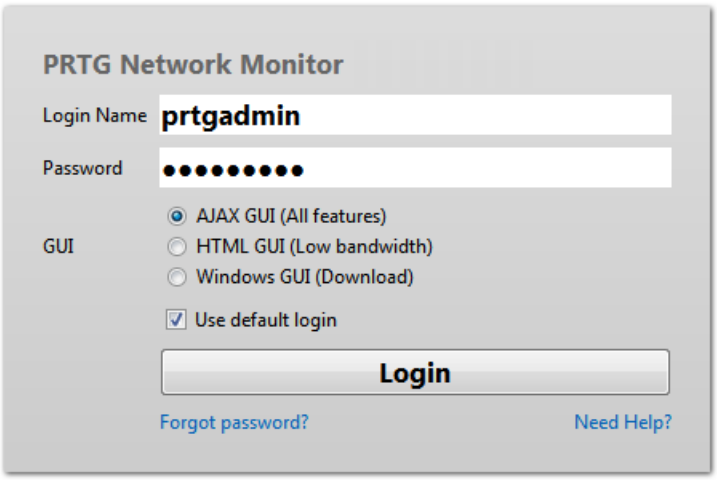
Example

As an example how to confirm an unknown certificate, find below a description for the most common web browsers:

- In **Google Chrome 5**, click on **Proceed anyway** every time you call the web interface.
- In **Mozilla Firefox 3**, click on **I Understand the Risks**, **Add Exception...**, **Get Certificate**; leave the check mark for **Permanently store this exception**; and finally click on **Confirm Security Exception**. You only have to go through this procedure once for every Firefox browser and PRTG core server.
- In **Internet Explorer 8** or **9**, click on **Continue to this website (not recommended)** every time you call the web interface. We recommend to not use Internet Explorer 8 or earlier.

Login

After loading the web interface, the login screen is shown:

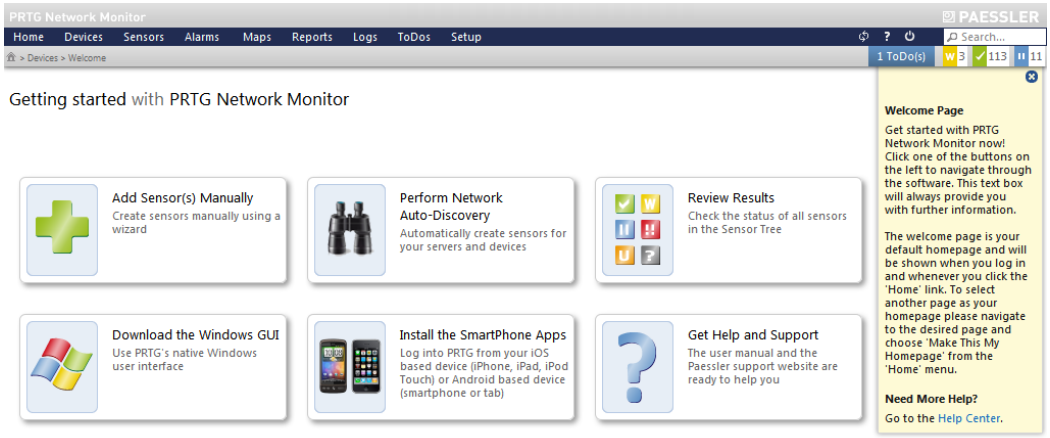


PRTG Login Screen

- Leave the default setting **AJAX GUI (All features)**.
- Click on **Use default login** to automatically fill in login name and password (both **prtgadmin**).
- Click on the **Login** button to proceed to the PRTG web interface.

2.3 THREE—Auto-Discover Your Network

Click on the **Home** button in main menu. The welcome screen is shown.

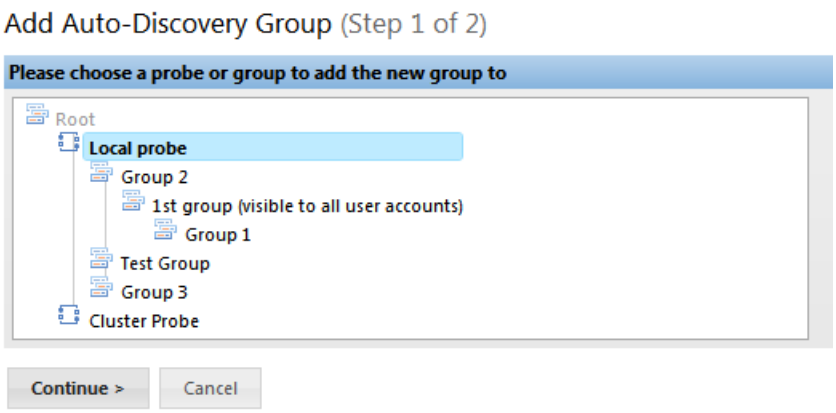

PRTG Network Monitor
PAESSLER
Home Devices Sensors Alarms Maps Reports Logs ToDos Setup
Search...
> Devices > Welcome
1 ToDo(s) 3 113 11
Getting started with PRTG Network Monitor
Add Sensor(s) Manually
Create sensors manually using a wizard
Perform Network Auto-Discovery
Automatically create sensors for your servers and devices
Review Results
Check the status of all sensors in the Sensor Tree
Download the Windows GUI
Use PRTG's native Windows user interface
Install the SmartPhone Apps
Log into PRTG from your iOS based device (iPhone, iPad, iPod Touch) or Android based device (smartphone or tab)
Get Help and Support
The user manual and the Paessler support website are ready to help you
Welcome Page
Get started with PRTG Network Monitor now! Click one of the buttons on the left to navigate through the software. This text box will always provide you with further information.
The welcome page is your default homepage and will be shown when you log in and whenever you click the 'Home' link. To select another page as your homepage please navigate to the desired page and choose 'Make This My Homepage' from the 'Home' menu.
Need More Help?
Go to the Help Center.

Welcome Screen

Click on **Network Auto-Discovery** to automatically scan in your network. PRTG will try to detect all attached devices automatically in just two steps. For video instructions, please see the More 34 section below.

Auto-Discovery—Step 1

In the first step, the tree with all probes and groups of your setup is shown.



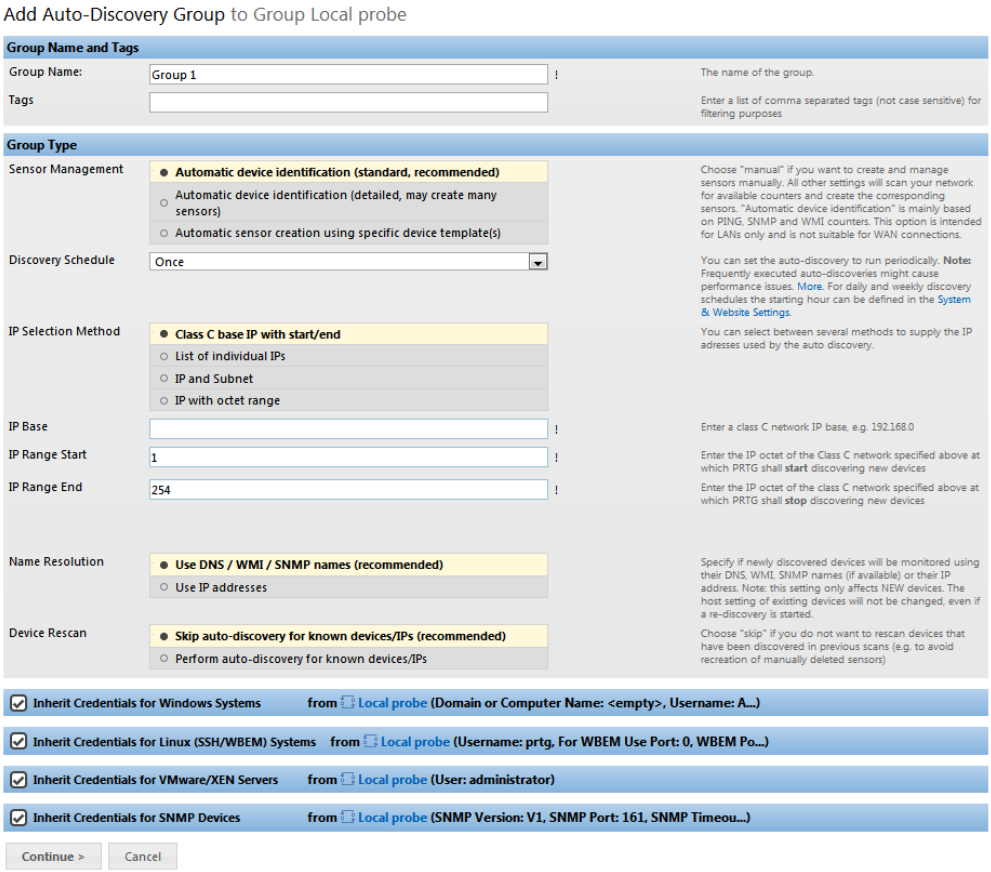
Add Auto-Discovery Group Assistent Step 1

- Choose **Local probe** from the device tree.
- Click the **Continue** button.

© 2011 Paessler AG

Auto-Discovery—Step 2

In the second step, some additional information about your network is required.


Add Auto-Discovery Group to Group Local probe
Group Name and Tags
Group Name:
Group 1
The name of the group.
Tags
Enter a list of comma separated tags (not case sensitive) for filtering purposes
Group Type
Sensor Management
Automatic device identification (standard, recommended)
Automatic device identification (detailed, may create many sensors)
Automatic sensor creation using specific device template(s)
Choose "manual" if you want to create and manage sensors manually. All other settings will scan your network for available counters and create the corresponding sensors. "Automatic device identification" is mainly based on PING, SNMP and WMI counters. This option is intended for LANs only and is not suitable for WAN connections.
Discovery Schedule
Once
You can set the auto-discovery to run periodically. Note: Frequently executed auto-discoveries might cause performance issues. More. For daily and weekly discovery schedules the starting hour can be defined in the System & Website Settings.
IP Selection Method
Class C base IP with start/end
List of individual IPs
IP and Subnet
IP with octet range
You can select between several methods to supply the IP adresses used by the auto discovery.
IP Base
Enter a class C network IP base, e.g. 192.168.0
IP Range Start
1
Enter the IP octet of the Class C network specified above at which PRTG shall start discovering new devices
IP Range End
254
Enter the IP octet of the class C network specified above at which PRTG shall stop discovering new devices
Name Resolution
Use DNS / WMI / SNMP names (recommended)
Use IP addresses
Specify if newly discovered devices will be monitored using their DNS, WMI, SNMP names (if available) or their IP address. Note: this setting only affects NEW devices. The host setting of existing devices will not be changed, even if a re-discovery is started.
Device Rescan
Skip auto-discovery for known devices/IPs (recommended)
Perform auto-discovery for known devices/IPs
Choose "skip" if you do not want to rescan devices that have been discovered in previous scans (e.g. to avoid recreation of manually deleted sensors)
Inherit Credentials for Windows Systems from Local probe (Domain or Computer Name: <empty>, Username: A...)
Inherit Credentials for Linux (SSH/WBEM) Systems from Local probe (Username: prtg, For WBEM Use Port: 0, WBEM Po...)
Inherit Credentials for VMware/XEN Servers from Local probe (User: administrator)
Inherit Credentials for SNMP Devices from Local probe (SNMP Version: V1, SNMP Port: 161, SNMP Timeou...)
Continue >
Cancel

Add Auto-Discovery Group Assistant Step 2

- With the **IP Selection Method**, choose whether you want to enter a **Class C base IP range**, a **List of individual IPs**, **IP and Subnet**, or **IP with octet range**. All of these methods result in an IP address range will will be scanned during the auto-discovery process. Based on your selection above, different setting fields are available.

- We recommend you leave the **Class C base IP** option. In the **IP Base** field, enter the first three octets of your network's IP range, for example **192.168.0** or **10.0.0**, or whatever IP address range you use. If you don't change the values for **IP Range Start** and **End**, PRTG will automatically complete the IP base and scan all IP addresses ending in *.1* to *.254*.

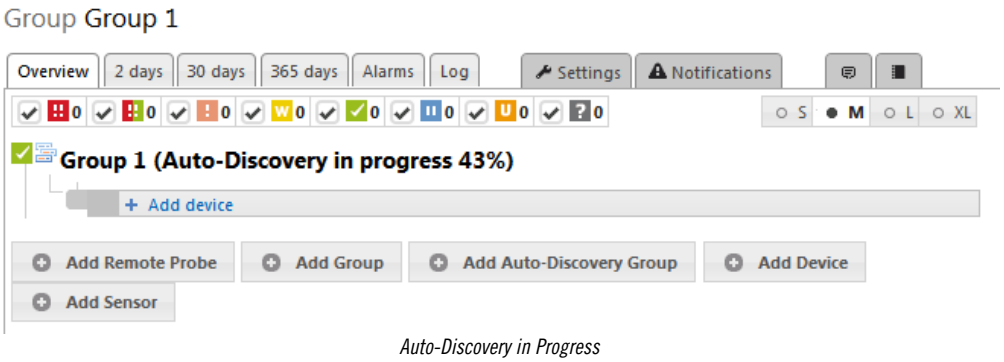
- If available, provide credentials for **Windows Systems**, **Linux Systems**, **VMware/XEN Servers**, and for **SNMP Devices**. You can show the respective settings by removing the check mark symbol at the beginning of the respective line. Find more information in the Auto-Discovery 145 section.

- Keep the default values for all other settings.

- Click the **Continue** button.

Ready

PRTG will now start discovering your network in the background, adding devices and sensors automatically. Meanwhile, you can get familiar with the Ajax web interface.



Auto-Discovery in Progress

The first steps are taken. Usually, the auto-discovery function has already detected most of the devices in your network. There are also sensors on the local **Probe Device**, monitoring the computer PRTG is installed on. In the welcome screen, click on **Review Results** to view the device tree with all devices.

As next step, we recommend going through the following sections:

- Ajax Web Interface 92
- Activating the Product 57
- Understanding the Basic Concepts 74
- Root Group Settings 166
- Device and Sensor Setup 144

More

Video Tutorial: There is a video available on the Paessler video tutorials page.

- http://www.paessler.com/support/video_tutorials

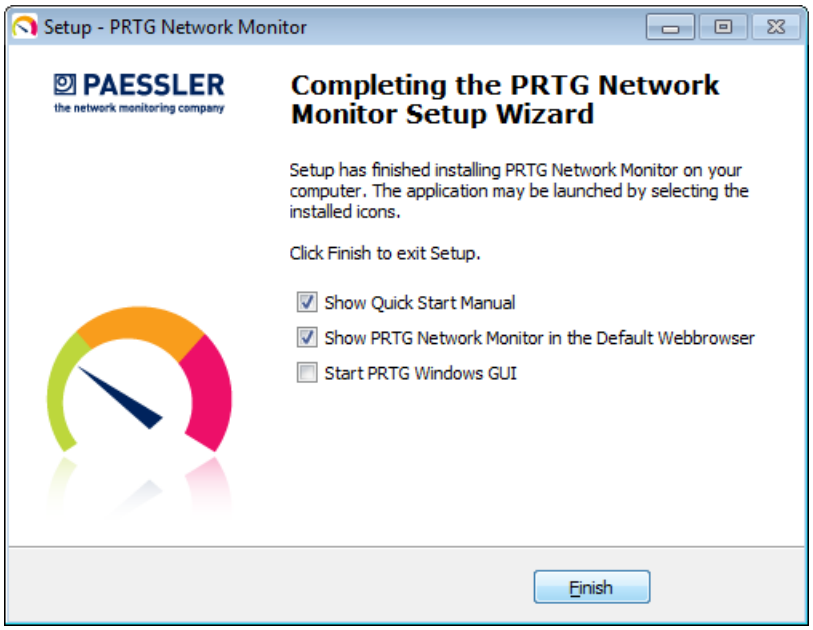
© 2011 Paessler AG

Part

Installing the Software

3 Installing the Software

This section describes how to download and install your PRTG product.


Setup - PRTG Network Monitor
PAESSLER
the network monitoring company
Completing the PRTG Network Monitor Setup Wizard
Setup has finished installing PRTG Network Monitor on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Show Quick Start Manual
Show PRTG Network Monitor in the Default Webbrowser
Start PRTG Windows GUI
Finish

PRTG Setup

Please see the following sections for more information.

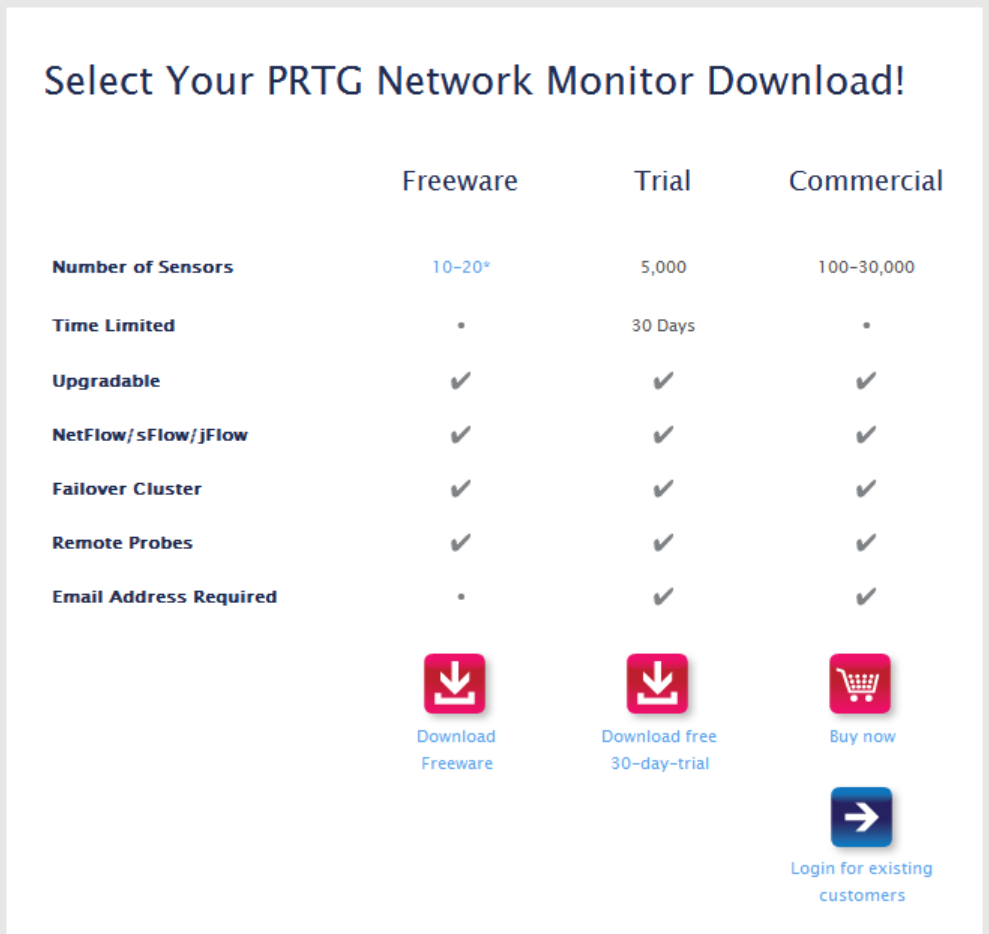
Installing the Software—Topics

- Download 37
- Upgrade From Previous Versions to V8 39
- Install a PRTG Core Server 41
- Install a PRTG Cluster 53
- Enter a License Key 55
- Activate the Product 57
- Install a PRTG Remote Probe 59
- Install the Windows GUI 64
- Uninstall 69

© 2011 Paessler AG

3.1 Download PRTG

On the Paessler website, you find two different installers for PRTG, a public download for the Freeware and Trial editions, and another download for the commercial editions (which is only available for paying customers).



PRTG Download at Paessler Website

Downloading the Freeware Edition or Trial Edition

Please download the latest publicly available file from the Paessler website. When downloading the Trial Edition, you can also request a trial key there:

- http://www.paessler.com/prtg/download

Downloading the Commercial Editions

Downloads and updates are free to customers with an active maintenance contract. Please log into the Paessler website to get the latest download. You can also find your license key there:

- http://www.paessler.com/login

If you do not have an active maintenance contract, please contact sales@paessler.com.

© 2011 Paessler AG

3.2 Upgrade From Previous Versions to V8

If you already have installed a previous software version, there are several possibilities for you.

Note: We recommend you always have a proper backup of your monitoring data and configuration. In most cases both will be maintained when upgrading. Anyway, we recommend a backup before upgrading. Please see More 39 section below.

Upgrade From Older Version 8.x Versions

If you have been running PRTG Network monitor with an earlier V8.x version number, simply install 41 the latest version on top of the previous version. Your configuration will be kept. If you have configured PRTG as a cluster, you only have to install an update on any node server (master or failover). The new version will then be deployed to the cluster automatically. *Note:* We recommend you always have a proper backup of your monitoring data.

Upgrade From PRTG Network Monitor 7

If you have been running PRTG V7, your configuration will be kept when installing PRTG in **Standalone Mode** or when installing a **Master Node**. *Note:* If you're using special custom sensors, these may not work with v8.

Only when installing a failover node on top of an existing PRTG 7 installation, the configuration cannot be kept and is written to a backup folder. Then, the new cluster configuration is received from the master node of the cluster. As all nodes work with the same configuration, a failover node's old configuration and monitoring data can no longer be used. If you want to keep a configuration of PRTG 7, please install the master node on top of the old installation and use other servers for the failover node installations. *Note:* We recommend you always have a proper backup of your monitoring data.

Upgrade From Older PRTG Products

For all other predecessor products, a direct data import into version 8 is not possible.

If you have been using IPCheck 5 or PRTG Traffic Grapher 6, we strongly recommend to perform a clean installation of PRTG 8 and set up your configuration anew. Using PRTG's auto-discovery is the easiest way to quickly configure a monitoring of your entire network. Please see Quick Start Guide 26 section for more information.

If you really need to import data from *PRTG Traffic Grapher Version 6* or *IPCheck Server Monitor Version 5*, you have to install PRTG 7 first and import data there. For those products, most of your data (monitoring setup and historic data) can be imported into PRTG 7. Importing data from earlier versions is not possible. For more information, please see the article in the More 39 section below.

More

Knowledge Base: How do I backup all data and configuration of my PRTG installation?
- http://www.paessler.com/knowledgebase/en/topic/523

Knowledge Base: How can I upgrade from previous PRTG versions to PRTG V8?

- http://www.paessler.com/knowledgebase/en/topic/9143

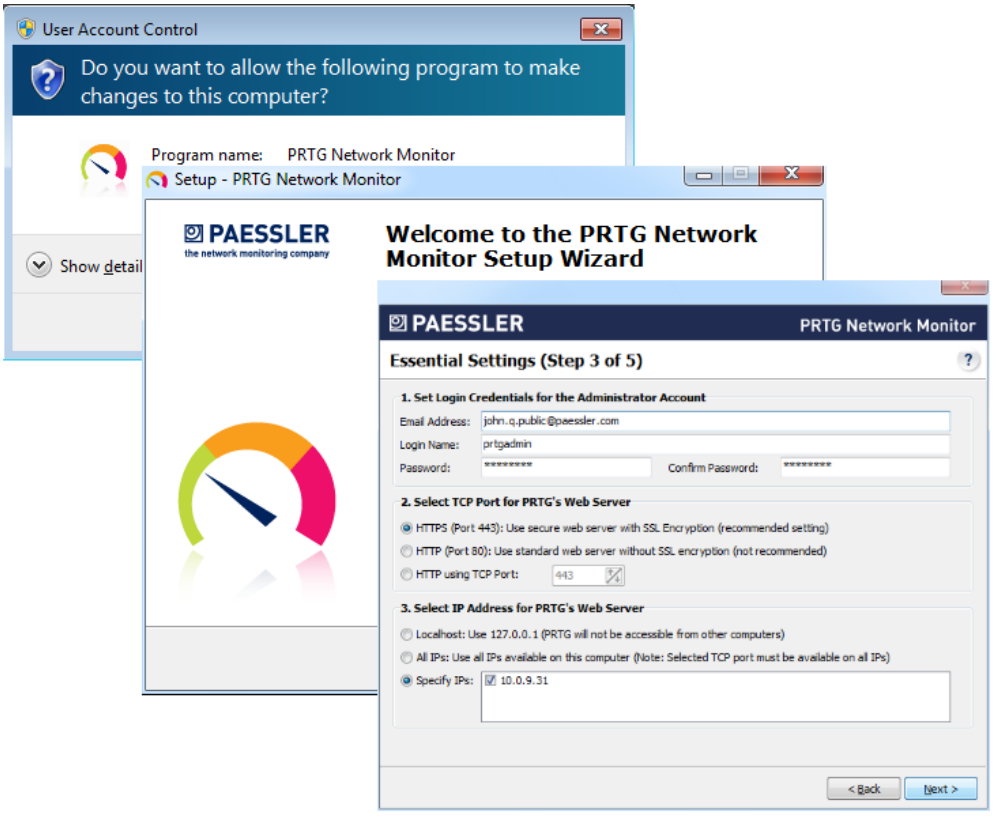
Knowledge Base: How do I Import Data from PRTG Traffic Grapher 6 or IPCheck Server Monitor 5 in PRTG Network Monitor?

- http://www.paessler.com/knowledgebase/en/topic/253

© 2011 Paessler AG

3.3 Install a PRTG Core Server

Installing PRTG is easy. The setup process will guide you through both installation and welcome wizard.

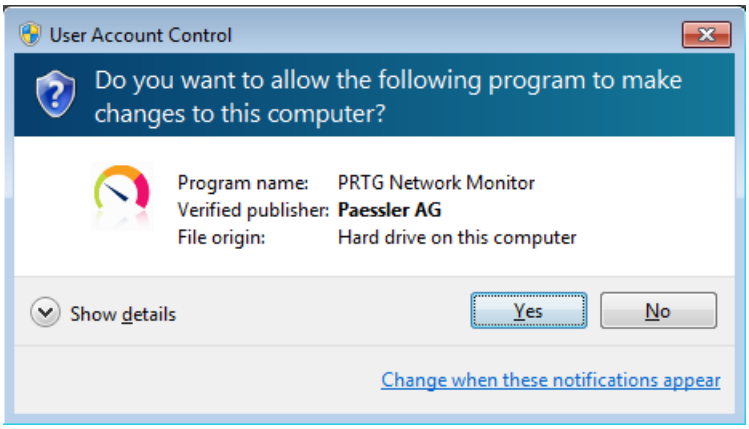

User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: PRTG Network Monitor
Show detail
Setup - PRTG Network Monitor
PAESSLER
the network monitoring company
Welcome to the PRTG Network Monitor Setup Wizard
PAESSLER
PRTG Network Monitor
Essential Settings (Step 3 of 5)
1. Set Login Credentials for the Administrator Account
Email Address: john.q.public@paessler.com
Login Name: prtgadmin
Password: ********
Confirm Password: ********
2. Select TCP Port for PRTG's Web Server
HTTPS (Port 443): Use secure web server with SSL Encryption (recommended setting)
HTTP (Port 80): Use standard web server without SSL encryption (not recommended)
HTTP using TCP Port: 443
3. Select IP Address for PRTG's Web Server
Localhost: Use 127.0.0.1 (PRTG will not be accessible from other computers)
All IPs: Use all IPs available on this computer (Note: Selected TCP port must be available on all IPs)
Specify IPs: 10.0.9.31
< Back
Next >

PRTG Installation

- Setup Wizard 42
- Welcome Wizard 45

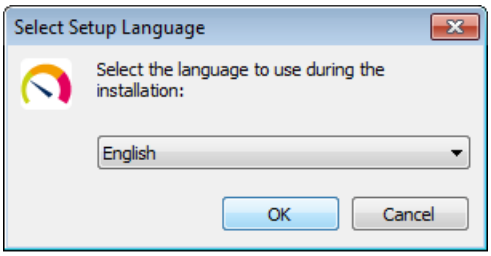
3.3.1 Setup Wizard

Installing the software is similar to other Windows-based applications. To install the application please run the installation setup program from the ZIP file that you have downloaded.


User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: PRTG Network Monitor
Verified publisher: Paessler AG
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

Windows User Account Control Confirmation Request

Confirm the question of the Windows User Account Control with **Yes** to allow the program to install. The usual software installation wizard will guide you through the installation process.



Setup Language Selection

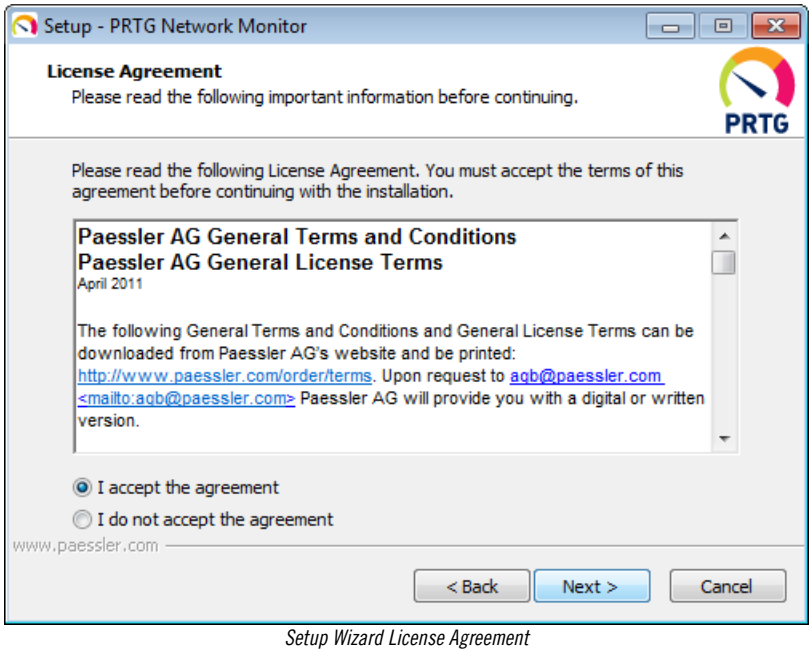
Please select a language for your product and click the **OK** button. The available language options depend on both your Windows version and the setup file.

© 2011 Paessler AG

Setup - PRTG Network Monitor
PAESSLER
the network monitoring company
Welcome to the PRTG Network Monitor Setup Wizard
This will install PRTG Network Monitor (Commercial-Edition) on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

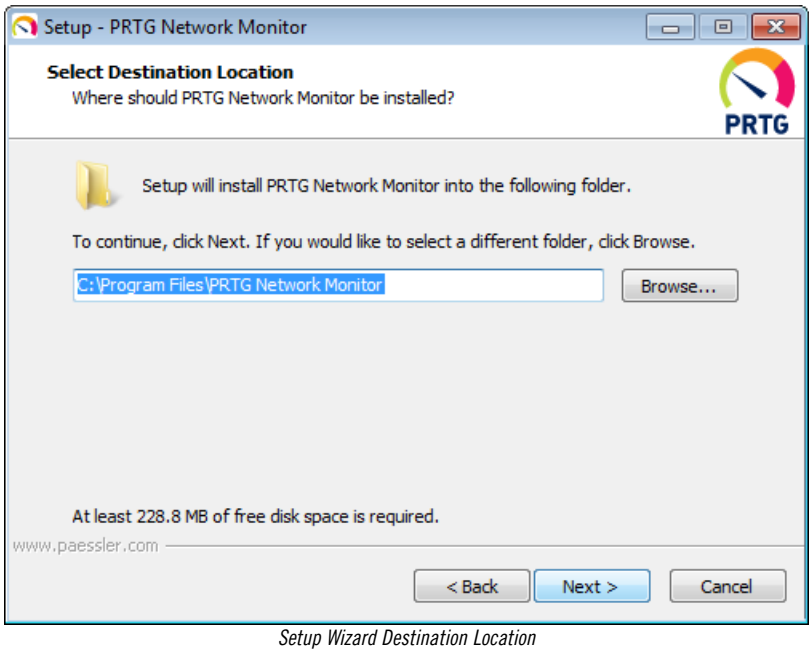
Setup Wizard Start Screen

Please click **Next** to walk through the wizard.


Setup - PRTG Network Monitor
License Agreement
Please read the following important information before continuing.
PRTG
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Paessler AG General Terms and Conditions
Paessler AG General License Terms
April 2011
The following General Terms and Conditions and General License Terms can be downloaded from Paessler AG's website and be printed: http://www.paessler.com/order/terms. Upon request to agb@paessler.com <mailto:agb@paessler.com> Paessler AG will provide you with a digital or written version.
I accept the agreement
I do not accept the agreement
www.paessler.com
< Back
Next >
Cancel

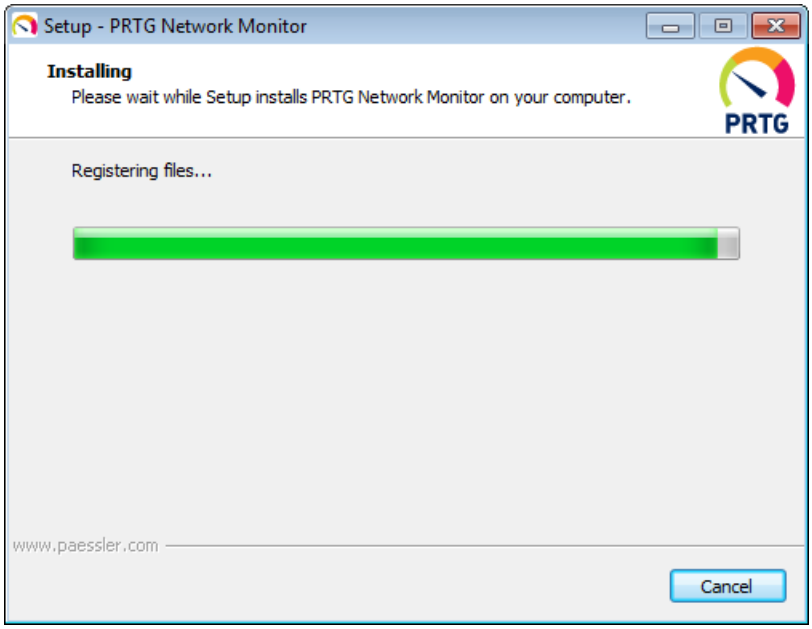
Setup Wizard License Agreement

After accepting the license agreement, you can choose the folder you wish to install the software in. We recommend using the default value.


Setup - PRTG Network Monitor
Select Destination Location
Where should PRTG Network Monitor be installed?
PRTG
Setup will install PRTG Network Monitor into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\PRTG Network Monitor
Browse...
At least 228.8 MB of free disk space is required.
www.paessler.com
< Back
Next >
Cancel

Setup Wizard Destination Location

As soon as you click **Next**, the necessary files will be copied to your disk.



Setup Wizard Installing

After installation, the Welcome Wizard 45 is shown if you're installing a major version for the first time.

© 2011 Paessler AG

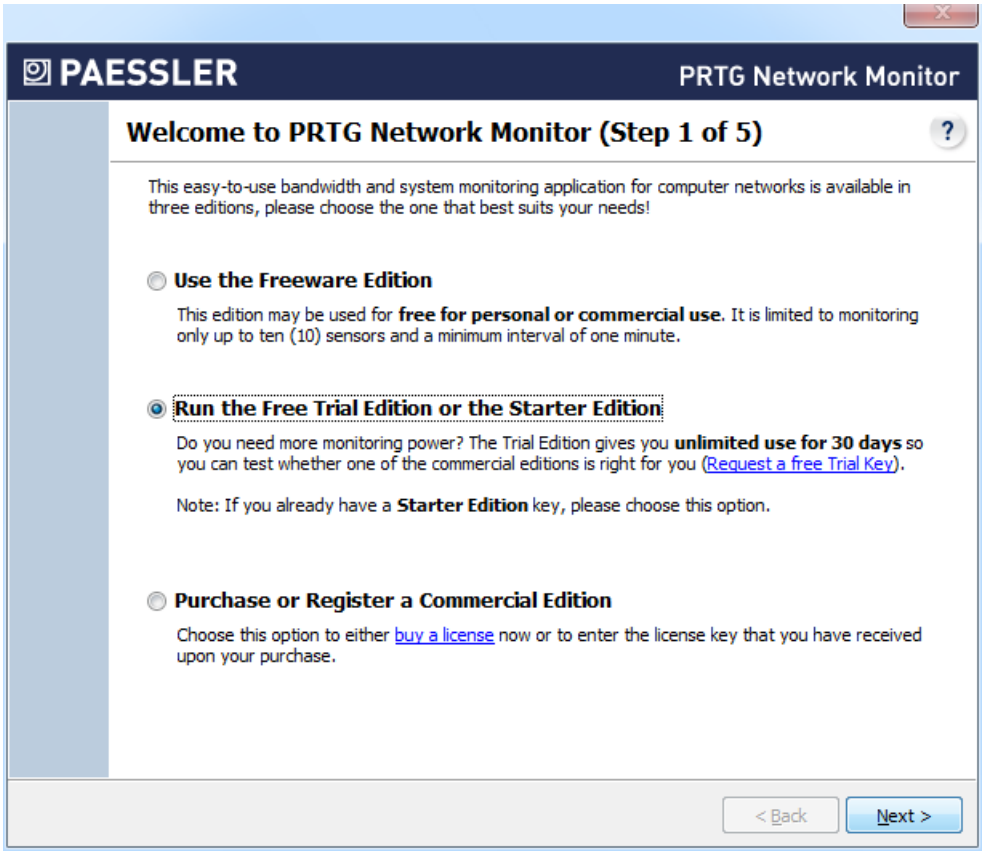
3.3.2 Welcome Wizard

Directly after installation, a welcome wizard appears. *Note:* When updating an existing V8 version of PRTG with a newer version of V8, this wizard is *not* shown.

Follow the welcome wizard by clicking on the **Next** button. To load a web page with extended help, click on the blue question mark **?** symbol in the upper right corner any time.

Select Edition

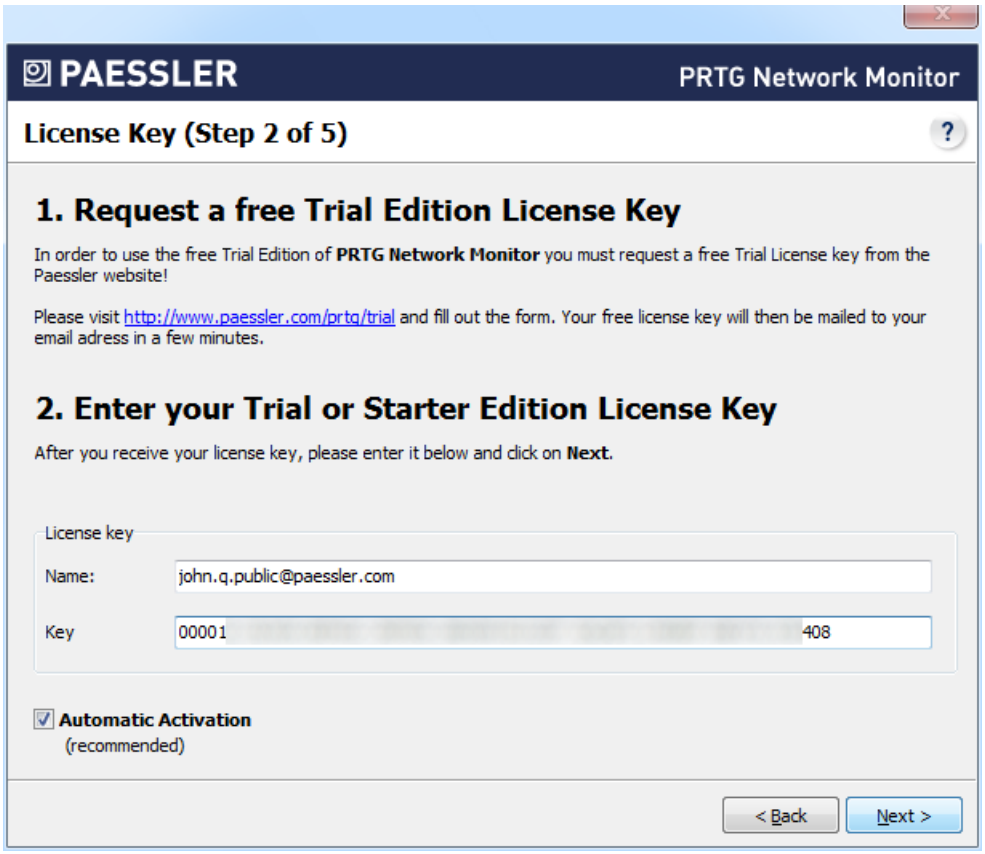
In step 1 of 5 a dialog appears, asking for the edition you would like to install. Please select the proper option.


PAESSLER
PRTG Network Monitor
Welcome to PRTG Network Monitor (Step 1 of 5)
This easy-to-use bandwidth and system monitoring application for computer networks is available in three editions, please choose the one that best suits your needs!
Use the Freeware Edition
This edition may be used for free for personal or commercial use. It is limited to monitoring only up to ten (10) sensors and a minimum interval of one minute.
Run the Free Trial Edition or the Starter Edition
Do you need more monitoring power? The Trial Edition gives you unlimited use for 30 days so you can test whether one of the commercial editions is right for you (Request a free Trial Key).
Note: If you already have a Starter Edition key, please choose this option.
Purchase or Register a Commercial Edition
Choose this option to either buy a license now or to enter the license key that you have received upon your purchase.
< Back
Next >

Welcome Wizard License Selection

Enter License Information

When selecting Trial Edition, Starter Edition (see More 52 section below), or Commercial Edition, enter your license information in step 2 of 5. The **Automatic Activation** option will activate your product automatically via an existing Internet connection on first startup.

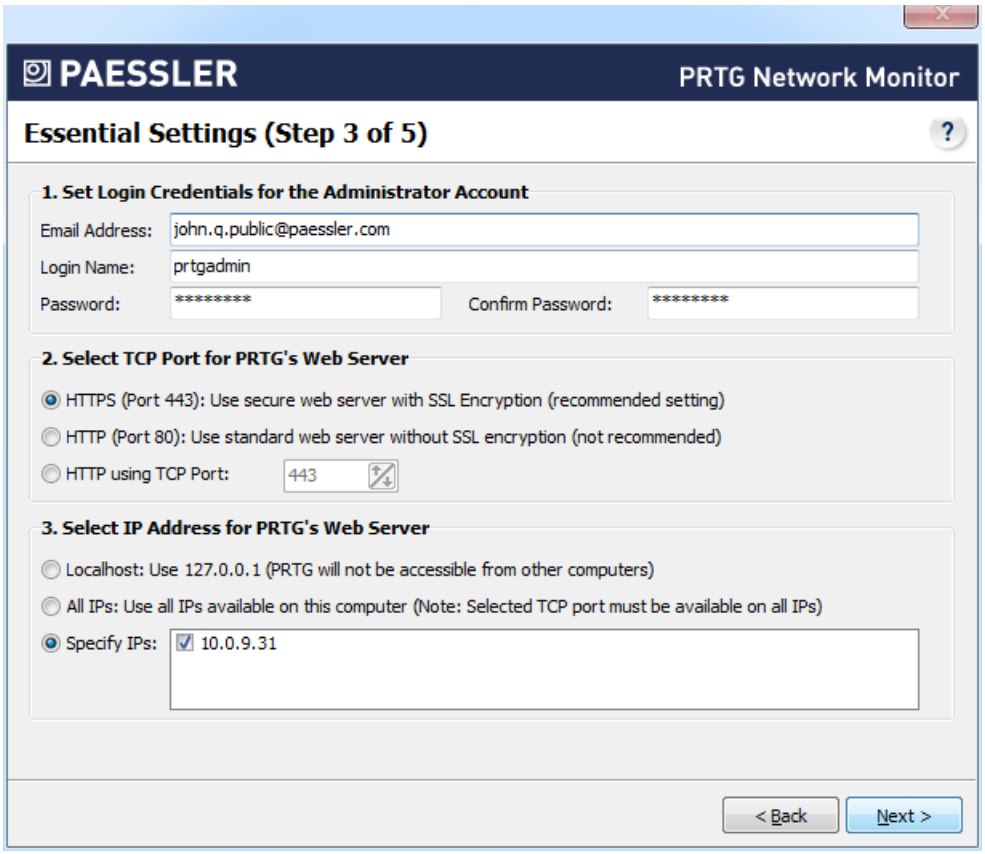

PAESSLER
PRTG Network Monitor
License Key (Step 2 of 5)
1. Request a free Trial Edition License Key
In order to use the free Trial Edition of PRTG Network Monitor you must request a free Trial License key from the Paessler website!
Please visit http://www.paessler.com/prtg/trial and fill out the form. Your free license key will then be mailed to your email adress in a few minutes.
2. Enter your Trial or Starter Edition License Key
After you receive your license key, please enter it below and click on Next.
License key
Name:
john.q.public@paessler.com
Key
00001
408
Automatic Activation
(recommended)
< Back
Next >

Welcome Wizard Trial License Key Input

Essential Settings

In step 3 of 5 please define important essential settings.

© 2011 Paessler AG


PAESSLER
PRTG Network Monitor
Essential Settings (Step 3 of 5)
1. Set Login Credentials for the Administrator Account
Email Address:
john.q.public@paessler.com
Login Name:
prtgadmin
Password:
Confirm Password:
2. Select TCP Port for PRTG's Web Server
HTTPS (Port 443): Use secure web server with SSL Encryption (recommended setting)
HTTP (Port 80): Use standard web server without SSL encryption (not recommended)
HTTP using TCP Port:
443
3. Select IP Address for PRTG's Web Server
Localhost: Use 127.0.0.1 (PRTG will not be accessible from other computers)
All IPs: Use all IPs available on this computer (Note: Selected TCP port must be available on all IPs)
Specify IPs:
10.0.9.31
< Back
Next >

Welcome Wizard Essential Settings

Essential Settings—1. Set Login Credentials for the Administrator Account

Enter the administrator's contact email address and define login credentials for PRTG.

Email Address

- Enter a valid administrator's email address.
- By default, PRTG will send notifications and important messages to this address.

Login Name

- Enter a name for the PRTG administrator login; this is your default login.
- It is used when logging in to the PRTG Web- or Windows interface.
- If you do not change this setting, the default login name **prtgadmin** is used.

Password

- Enter a password for the PRTG administrator login; this is your default login.
- It is used when logging in to the PRTG Web- or Windows interface.
- If you do not change this setting, the default password **prtgadmin** is used.

Confirm Password

- Re-enter the password for the PRTG administrator login.

- If you do not change this setting, the default password **prtgadmin** is used.

Essential Settings—2. Select TCP Port for PRTG's Web Server

PRTG is running a web server in order to provide the web and Windows interface. Please specify on which port this web server will run.

HTTPS (Port 443)

- This is the recommended setting.
- Use a secure HTTPS connection that is encrypted via SSL on port 443.
- SSL-secured connections can be established on port 443 only.
- *Note:* Although the connection is secure, you will see a certificate warning in your browser when logging in to the PRTG web interface, because the default certificate is unknown to your browser. You can install another SSL certificate for PRTG later. Please see the More 52 section below.
- *Note:* If port 80 is free, PRTG will reserve it as well. When users try to connect on port 80 via HTTP, they will then be redirected to port 443 via HTTPS. You can change this behavior later. Please see the More 52 section below.

HTTP (Port 80)

- This setting is not recommended for WAN connections.
- Use a standard web server without SSL encryption on port 80.
- *Note:* If used on the Internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend using this option in a LAN only.

HTTP using TCP Port

- This setting is not recommended for WAN connections.
- Use a standard web server without SSL encryption on a custom port.
- This option is intended for systems with an existing web server.
- Enter the desired TCP port you want the PRTG web server to run on.
- *Note:* If used on the Internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend using this option in a LAN only.

Essential Settings—3. Select IP Address for PRTG's Web Server

PRTG is running a web server in order to provide access via the web and Windows interface. Please specify which IP address this web server will run on. *Note:* Later, you can log into PRTG by simply pointing your browser to the specified IP address.

Localhost

- Use *127.0.0.1* only.
- PRTG's web and Windows interface will only be accessible from the computer PRTG is installed on.
- *Note:* Either the selected port or at least one port in the range from **8080** to **8089** has to be available on *127.0.0.1*.

All IPs

- Use all IP addresses available on this computer and enable access to the web server for all of these addresses.
- *Note:* The TCP port selected above must be free on every available IP address.

© 2011 Paessler AG

Specify IPs

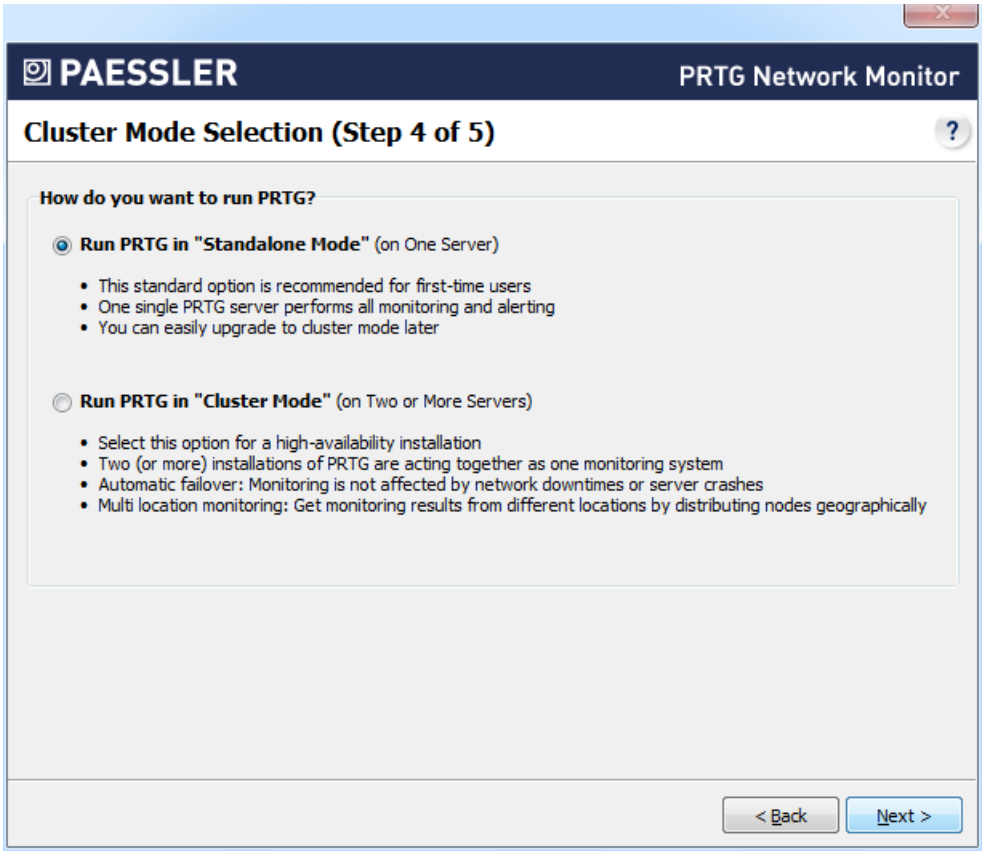
- Select specific IP addresses on which the PRTG Web server will run on.
- A list specific to your system is shown.
- Add a check mark in front of every IP address you want the PRTG web server to be available at.
- *Note:* Either the selected port or at least one port in the range from **8080** to **8089** has to be available on the specified IP address.

Note: Regardless of the selected setting above, one port in the range from **8080** to **8180** has to be available on the specified IP address so PRTG can create reports. The report engine will try to connect to the core server on one of these ports.

Welcome Wizard—Cluster Mode Selection

PRTG offers single failover clustering in all licenses—even using the Freeware edition. For detailed instructions, please see Install a PRTG Cluster 53 section.

In step 4 of 5, please select if you want to configure PRTG for a cluster.


PAESSLER
PRTG Network Monitor
Cluster Mode Selection (Step 4 of 5)
How do you want to run PRTG?
Run PRTG in "Standalone Mode" (on One Server)
This standard option is recommended for first-time users
One single PRTG server performs all monitoring and alerting
You can easily upgrade to cluster mode later
Run PRTG in "Cluster Mode" (on Two or More Servers)
Select this option for a high-availability installation
Two (or more) installations of PRTG are acting together as one monitoring system
Automatic failover: Monitoring is not affected by network downtimes or server crashes
Multi location monitoring: Get monitoring results from different locations by distributing nodes geographically
< Back
Next >

Welcome Wizard Cluster Mode Selection

Run PRTG in "Standalone Mode"

- Run one instance of PRTG as a standalone solution.

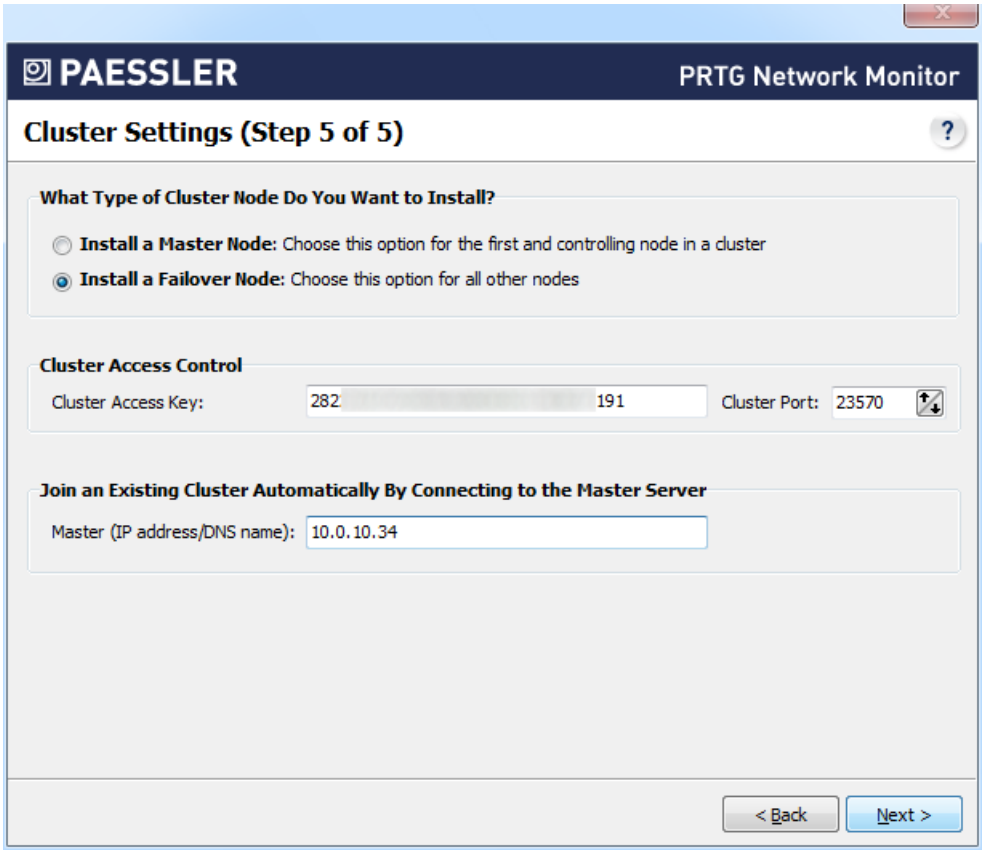
- If you are not sure what to choose, take this option. You can integrate a PRTG installation in standalone mode into a cluster later on.
- Monitoring and alerting is performed by one single PRTG installation only.

Run PRTG in "Cluster Mode"

- Run several PRTG installations combined in a cluster.
- Select this option for a high-available monitoring solution.
- Two or more PRTG installations work together in one cluster and act as one monitoring system.
- Automatic failover: One PRTG installation takes over monitoring and alerting seamlessly in case the other installation fails or the server is restarted.
- Multi-location monitoring: You also have the option to monitor your network from different locations by setting up geographically distributed installations.
- For detailed instructions please see Install a PRTG Cluster 53 section.

Welcome Wizard—Cluster Settings

This screen only appears if you have chosen to set up a PRTG cluster. Please select whether you want this PRTG installation to be the master node or a failover node. For detailed instructions please see Install a PRTG Cluster 53 section.


PAESSLER
PRTG Network Monitor
Cluster Settings (Step 5 of 5)
What Type of Cluster Node Do You Want to Install?
Install a Master Node: Choose this option for the first and controlling node in a cluster
Install a Failover Node: Choose this option for all other nodes
Cluster Access Control
Cluster Access Key:
282
191
Cluster Port:
23570
Join an Existing Cluster Automatically By Connecting to the Master Server
Master (IP address/DNS name):
10.0.10.34
< Back
Next >

Welcome Wizard Cluster Settings

Install a Master Node

© 2011 Paessler AG

- Make this PRTG installation the master node of your cluster.
- Choose this option if you are about to make the first installation in your cluster.
- The master node usually controls your whole cluster.
- There may only be *one* master node in a PRTG cluster. Please do not install several master nodes, as they won't be able to connect to each other. Instead, use failover nodes for all other installations in your cluster.

Cluster Access Control (Master)

- **Cluster Access Key**: For safety reasons, a node can only connect to the cluster with a cluster access key. With the setup of the master node you will define a new key for the cluster here. The access key is already pre-defined; you can leave the default value.
- **Cluster Port**: All communication in the cluster is directed through the cluster port. It is already pre-defined; you can leave the default value.
- Please make sure the security settings in your network allow communication between all nodes on the defined port.
- Save both cluster access key and cluster port in a text file for later use; you will need them in the cluster settings for each failover node later.

Install a Failover Node

- Make this PRTG installation a failover node in the cluster.
- Choose this option if you have already set up a master node and want to add a failover node to your cluster.
- There may be several failover nodes in one cluster—provided that you have the appropriate license.

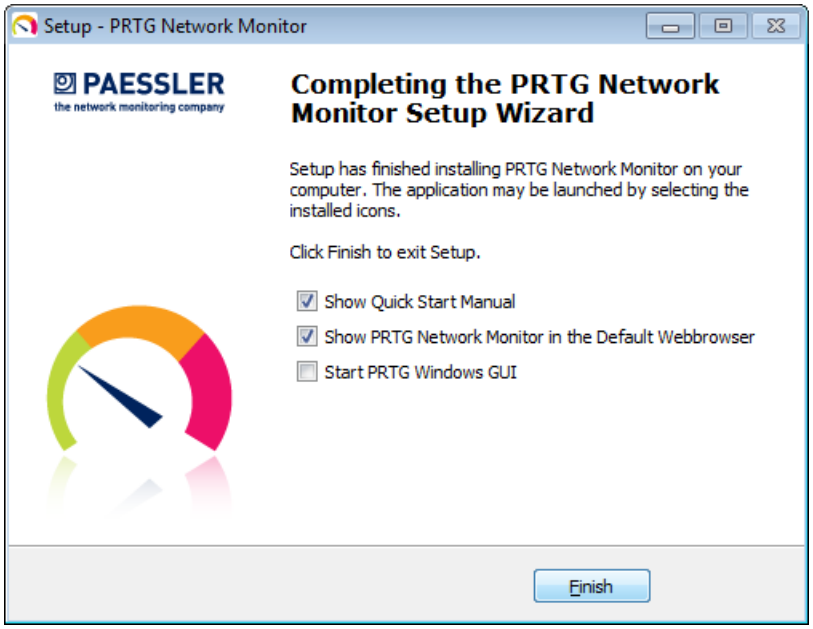
Cluster Access Control (Failover)

- **Cluster Access Key**: For safety reasons, a node can only connect to the cluster with a cluster access key. For a failover node, please enter the existing key you have defined while setting up the master node.
- **Cluster Port**: All communication in the cluster is directed through the cluster port. It must be the same port defined for the master node.
- Please make sure the security settings in your network allow communication between all nodes on the defined port.
- If unknown, you can look up cluster access key and cluster port in the **PRTG Server Administrator** program (**Cluster** tab) on the server your master node is running on.

Join an Existing Cluster Automatically

- This will add the failover node to the master node's settings automatically.
- **Master**: Enter the IP address or DNS name of the master node in order to join the cluster automatically.
- If you enter nothing here, you'll have to add the master node's IP address or DNS name later in the **PRTG Server Administrator** program on the server the failover node is running on. For more information, please see **Step 3** and following of *10 Steps to Set Up a PRTG Cluster—Scenario 3* (see More 52 section below).
- *Important:* After joining, you must confirm the new node in the master node's settings in order for the failover node to connect to the master node! For more information, please see **Step 7** and following of *10 Steps to Set Up a PRTG Cluster—Scenario 3* (see More 52 section below).

Finished


Setup - PRTG Network Monitor
PAESSLER
the network monitoring company
Completing the PRTG Network Monitor Setup Wizard
Setup has finished installing PRTG Network Monitor on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Show Quick Start Manual
Show PRTG Network Monitor in the Default Webbrowser
Start PRTG Windows GUI
Finish

Welcome Wizard Completed

Click on **Finish** to load the web interface 92.

More

Knowledge Base: What is the PRTG Starter Edition license?
- http://www.paessler.com/knowledgebase/en/topic/8063

Knowledge Base: How can I establish a secure web interface connection to PRTG?
- http://www.paessler.com/knowledgebase/en/topic/273

Knowledge Base: PRTG blocks port 80 although I'm using SSL on port 443. How to free port 80?
- http://www.paessler.com/knowledgebase/en/topic/5373

Knowledge Base: How do I set up a cluster in PRTG 8?
- http://www.paessler.com/knowledgebase/en/topic/6143

Knowledge Base: 10 Steps to Set Up a Cluster—Scenario 3
- http://www.paessler.com/knowledgebase/en/topic/6923

© 2011 Paessler AG

3.4 Install a PRTG Cluster

PRTG offers single failover clustering in all licenses—even using the freeware edition. A single failover cluster consists of two servers ("Node 1" and "Node 2"), each of them running one installation of PRTG. They are connected to each other and exchange configuration and monitoring data.

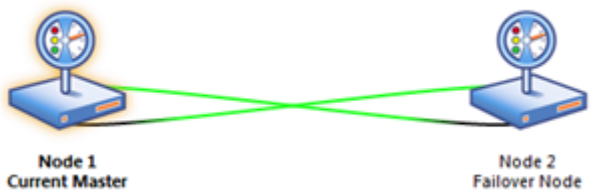


Illustration of a Single Failover Cluster

For setting up a cluster you need two or more (virtual) servers and there is one core installation 41 process necessary on each of them—with different options selected for each type of node. In return, you benefit from seamless high-available monitoring with automatic failover and/or multi-location monitoring.

In a cluster, you can install:

- **1 Master Node**
  On the master node, you set up your devices and configuration. Also notifications, reporting, and many other things are handled by the master node.

- **Up to 4 Failover Nodes**
  You can install one, two, three, or four additional nodes for fail-safe, gapless monitoring. Each of these nodes can monitor the devices in your network independently, collecting their own monitoring data. The data can be reviewed in a summarized way, enabling you to compare monitoring data from different nodes.

Start with setting up your master node. You can install additional failover nodes in a second step.

Before Getting Started

Configuring a cluster with one failover node is the most common way to set up a seamless network monitoring with PRTG. You will need two servers running any Windows version (XP/2003 or later); your servers can be real hardware or virtual machines.

Please make sure the following:

- Your servers must be up and running
- Your servers must be similar in regard to the system performance and speed (CPU, RAM memory, etc.)
- We recommend installing PRTG on dedicated systems for best performance
- Please bear in mind that a server running a cluster node may in rare cases be rebooted automatically without notice (e.g. for special software updates)
- Both servers must be visible for each other through the network

- Communication between the two servers must be possible in *both directions*. Please make sure that no software- or hardware firewall is blocking communication. All communication between nodes in the cluster is directed through one specific TCP port. You will define it during cluster setup (by default, it is **TCP port 23570**).
- A Failover Master will send notifications in case the Primary Master is not connected to the cluster. In order for mail
- Make your servers safe! From every cluster node, there is full access to all stored credentials as well as other configuration data and the monitoring results of the cluster. Also, PRTG software updates can be deployed through every node. So, please make sure you take security precautions to avoid security attacks (hackers, Trojans, etc.). You should secure every node server the same careful way as the master node server.

The Three Scenarios

There are different starting points for setting up a cluster. Each of them requires different instructions. Please see the following Knowledge Base articles.

Scenario 1: You do not have a PRTG 8 installation yet

Make a fresh installation of two PRTG version 8 servers as a cluster or integrate one existing PRTG version 7 server into a cluster of two PRTG version 8 installations.

- http://www.paessler.com/knowledgebase/en/topic/6903

Scenario 2: You've set up one PRTG 8 installation in single mode already

Integrate an existing PRTG version 8 server into a failover cluster with two PRTG version 8 installations.

- http://www.paessler.com/knowledgebase/en/topic/6913

Scenario 3: You've set up two PRTG 8 installations already, each running in single mode

Combine two existing PRTG version 8 servers into one failover cluster. The cluster will take over the configuration of *one* server (the future master server); the configuration of the other server (the future failover node) will be discarded.

- http://www.paessler.com/knowledgebase/en/topic/6923

More

Knowledge Base: How do I set up a cluster in PRTG 8?

- http://www.paessler.com/knowledgebase/en/topic/6143

Knowledge Base: What's the Clustering Feature in PRTG 8?

- http://www.paessler.com/knowledgebase/en/topic/6403

Knowledge Base: What is a Failover Master and how does it behave?

- http://www.paessler.com/knowledgebase/en/topic/7663

Knowledge Base: PRTG 8 Cluster: How do I convert a (temporary) Failover Master node to be the Primary Master node?

- http://www.paessler.com/knowledgebase/en/topic/8053

© 2011 Paessler AG

3.5 Enter a License Key

A license key for PRTG Network Monitor consists of the license name and a license key, which is a string that contains 70 characters and numbers. This information is usually sent to customers via email.

Example of license information

License Name: **John Q. Public**
License Key: **0223515-FFSEJC-ZHGRDFM-UR1CS8-U73FGK-G645F2-YVF1DD-H8323N-D11HG9-M2DRG**

You can either enter the license key during the installation process or you can select the **Use the Freeware Edition** option. When installing as Freeware, you can use the **PRTG Server Administrator** Windows program to enter a license key later. Your Freeware version will then be converted to a trial or commercial version. *Note:* You do not need to enter a license key if you want to use the freeware edition only.

Please check first if you have installed the proper edition and then enter the license key.

Step 1: Make Sure You Have Installed the Correct Edition

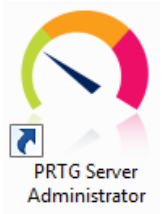
There are two different installers available for PRTG (see Download 37 section):

- The publicly available installer only contains the Freeware, Starter and Trial Editions
- The Commercial installer is only available for download for paying customers.

The Commercial Installer must be installed to run the commercial editions of PRTG Network Monitor. **If you have purchased a license key for PRTG you must download and install the latest Commercial Installer from the Paessler website in order to apply your license key.**

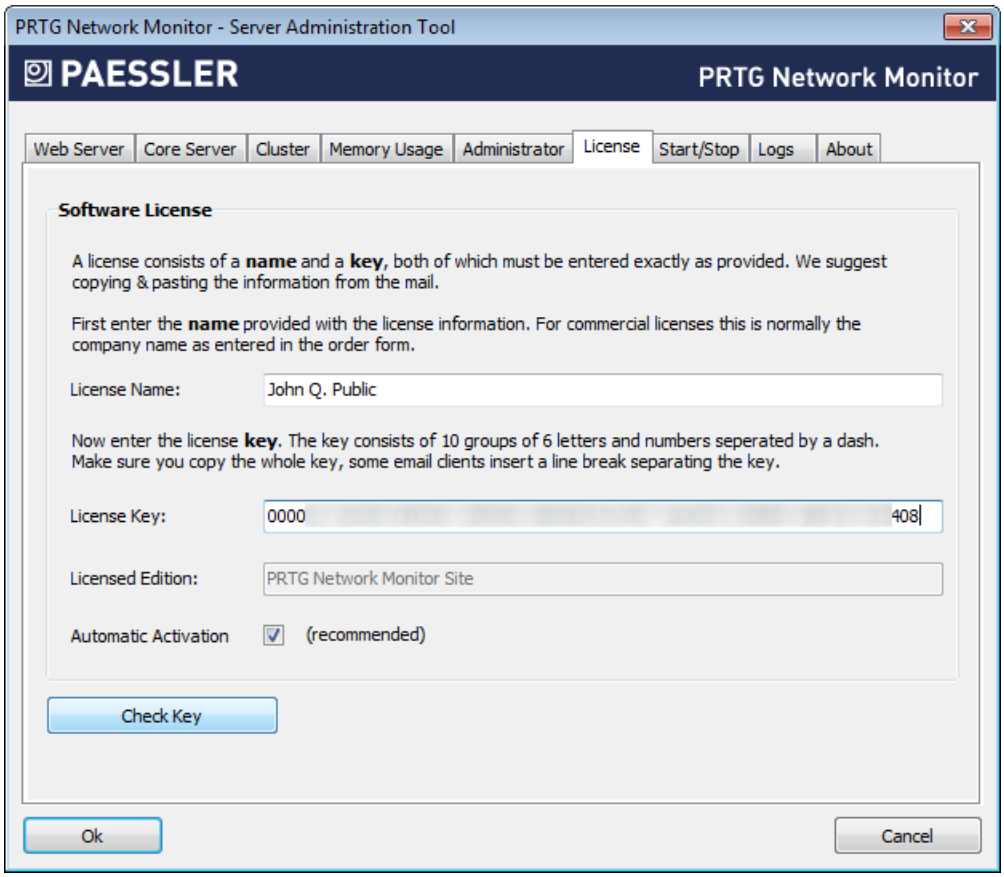
Step 2: Enter the License Key in the PRTG Server Administrator

Please start the **PRTG Server Administrator** program from the Windows Start Menu. In the program, select the **License** tab.



Start Menu Icon

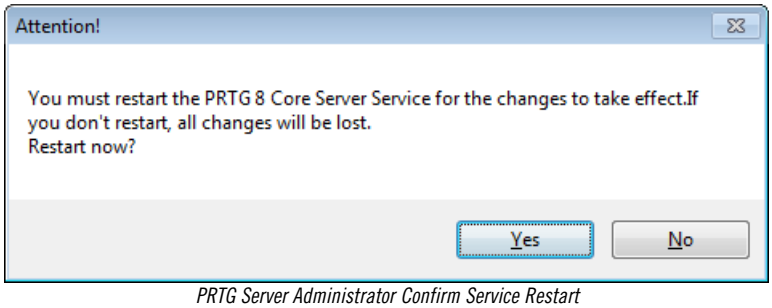
To use a PRTG license with this installation of PRTG, please enter the license information you have received from Paessler via email. To avoid typing errors, please copy and paste the name and the key from the email.


PRTG Network Monitor - Server Administration Tool
PAESSLER
PRTG Network Monitor
Web Server
Core Server
Cluster
Memory Usage
Administrator
License
Start/Stop
Logs
About
Software License
A license consists of a name and a key, both of which must be entered exactly as provided. We suggest copying & pasting the information from the mail.
First enter the name provided with the license information. For commercial licenses this is normally the company name as entered in the order form.
License Name:
John Q. Public
Now enter the license key. The key consists of 10 groups of 6 letters and numbers seperated by a dash. Make sure you copy the whole key, some email clients insert a line break separating the key.
License Key:
0000
408
Licensed Edition:
PRTG Network Monitor Site
Automatic Activation
(recommended)
Check Key
Ok
Cancel

PRTG Server Administrator License Tab

To make sure your key has been entered correctly please click on the **Check Key** button. A popup box will either show success or denial of your license information. In the **Licensed Edition** field you will see an accepted licence key. Please remember to activate your license in the web interface. For more details, please see Activate the Product 57 section.

Click on the **Ok** button to save and confirm to restart the core server service by clicking on the **Yes** button.

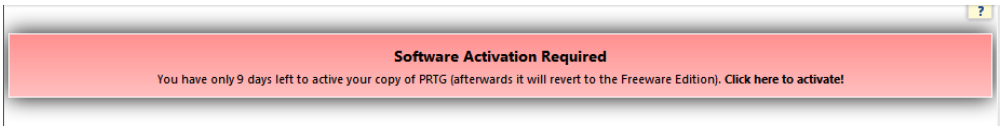

Attention!
You must restart the PRTG 8 Core Server Service for the changes to take effect.If you don't restart, all changes will be lost.
Restart now?
Yes
No

PRTG Server Administrator Confirm Service Restart

© 2011 Paessler AG

3.6 Activate the Product

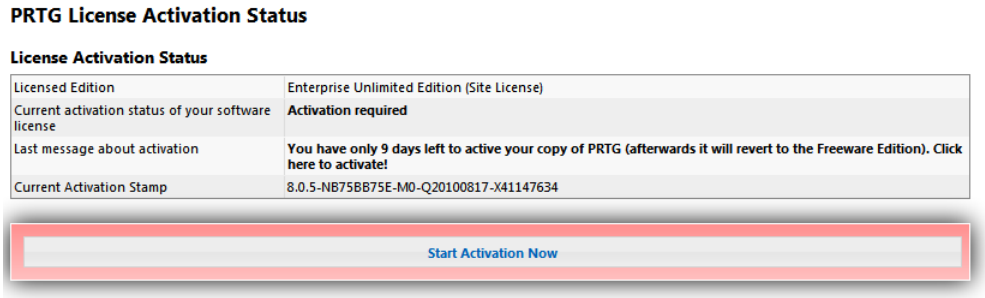
After installing the PRTG software and entering a license key, you have to run through the product activation process once in order to use it continuously (only Freeware and Trial Edition are activated automatically and do not require a special procedure). The activation has to be done within ten days after installation and only takes a few minutes. If you do not activate PRTG for ten days, it will temporarily revert to the Freeware Edition (with a maximum of 10 sensors) until you activate. Login to the PRTG web interface 94 to activate.


Software Activation Required
You have only 9 days left to active your copy of PRTG (afterwards it will revert to the Freeware Edition). Click here to activate!

Software Activation Information Box

Activate via Internet

In the PRTG web interface, choose **Setup | PRTG Status | Activation Status** from the main menu.


PRTG License Activation Status
License Activation Status
Licensed Edition
Enterprise Unlimited Edition (Site License)
Current activation status of your software license
Activation required
Last message about activation
You have only 9 days left to active your copy of PRTG (afterwards it will revert to the Freeware Edition). Click here to activate!
Current Activation Stamp
8.0.5-NB75BB75E-M0-Q20100817-X41147634
Start Activation Now

License Activation Status

Click on the button **Start Activation Now** to start product activation. PRTG will now connect with Paessler license server to check your license. A few seconds later you should see **Activation OK** in the License Activation Status.

Note: The PRTG core server need a direct Internet connection to activate. Proxy connections are not supported for activation. In case activation fails, you can activate via email.

Activate via Email

In the PRTG Web Interface, choose **Setup | PRTG Status | Activation Status** from the main menu.

If there is no Internet connection available, you can activate PRTG via email. To do so, first click on the **Start Activation Now** button. You will then see **Last message about activation: Activation failed** in the License Activation Status.

- Once the activation via Internet fails, the activation via email is available.
- Click on the **Start Activation per EMail** tab. You will see an **Activation Request Code**.
- Copy it and send it to the email address shown.

- Within two business days you will receive an email reply from Paessler, containing an activation code.
- Once you've received this email, go the **Finalize Activation per EMail** tab and copy the activation code into the according field.
- Click on **Confirm Activation**.

A few seconds later you should see **Activation OK** in the License Activation Status.

© 2011 Paessler AG

3.7 Install a PRTG Remote Probe

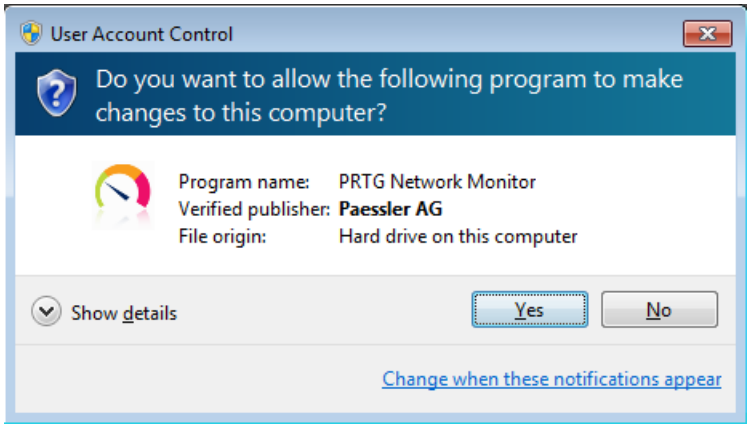
The local probe is already included in a PRTG core server installation [41]. You can install additional remote probes on other computers to relieve the core installation or to extend monitoring to distributed networks. *Note:* You cannot install a remote probe on a system already running a PRTG core installation.

Download Remote Probe Installer from the Web Interface

The remote probe version has to fit the PRTG core server version you will connect to. In order download your setup program to the computer you want to install it on, please connect to the Ajax web interface [93]. In the login screen [94], enter login name and password and from the main menu, select **Setup | Downloads | Remote Probe Installer**. Click on the **Download: Remote Probe Installer** button. You browser will show a download dialog. Save the setup program to your local hard disk drive.

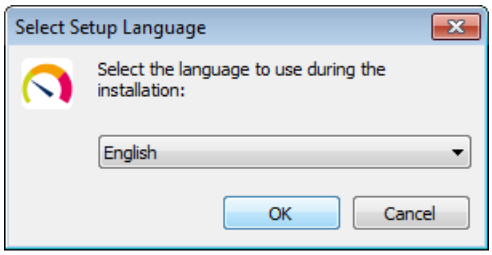
Install Remote Probe

Please execute the installation setup program you've just downloaded.


User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: PRTG Network Monitor
Verified publisher: Paessler AG
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

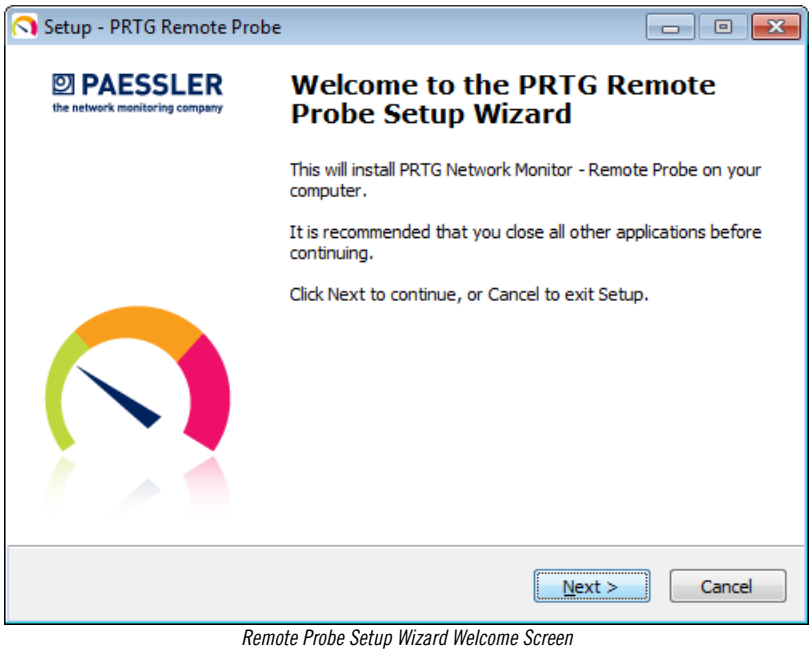
Windows User Account Control Confirmation Request

Confirm the question of the Windows User Account Control with **Yes** to allow the program to install. The usual software installation wizard will guide you through the installation process.



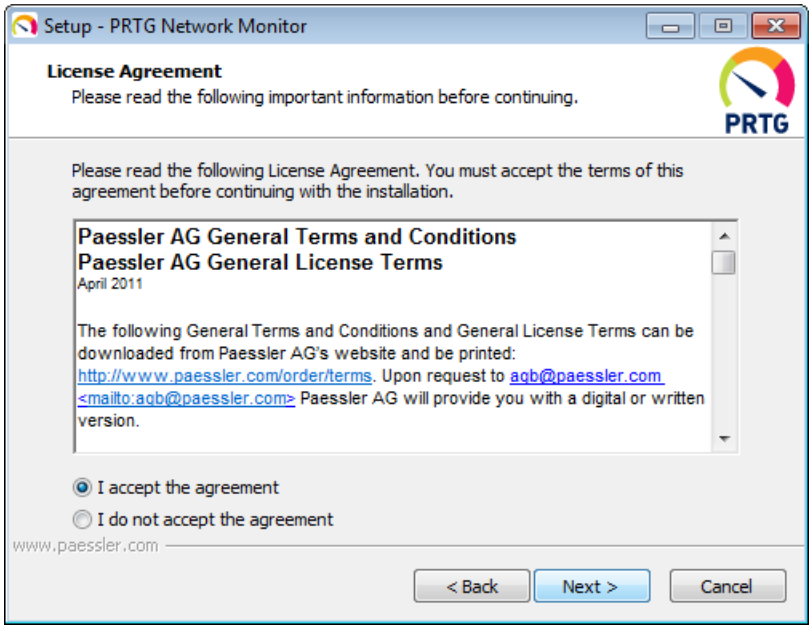
Setup Language Selection

Please select a language for your product and click the **OK** button. The available language options depend on both your Windows version and the setup file.


Setup - PRTG Remote Probe
PAESSLER
the network monitoring company
Welcome to the PRTG Remote Probe Setup Wizard
This will install PRTG Network Monitor - Remote Probe on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

Remote Probe Setup Wizard Welcome Screen

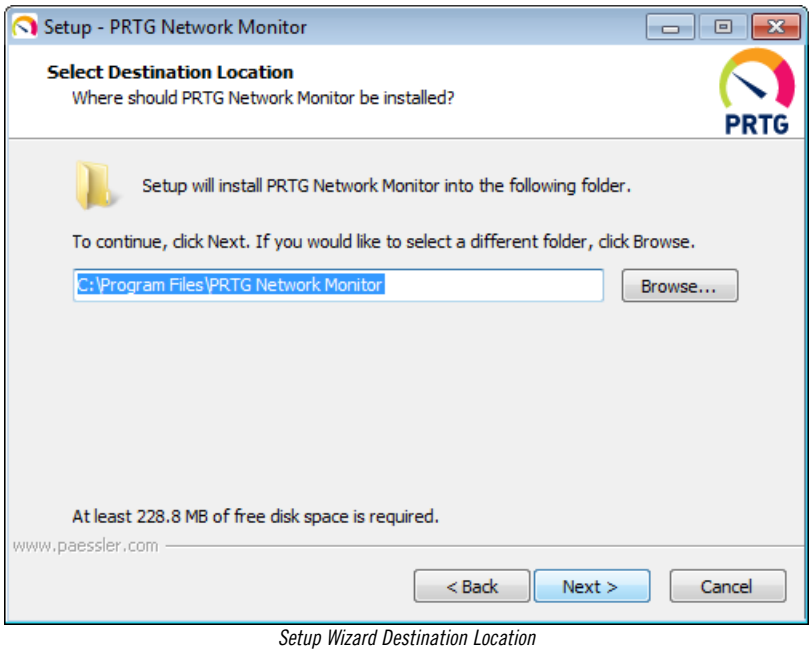
Please click **Next** to walk through the wizard.


Setup - PRTG Network Monitor
License Agreement
Please read the following important information before continuing.
PRTG
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Paessler AG General Terms and Conditions
Paessler AG General License Terms
April 2011
The following General Terms and Conditions and General License Terms can be downloaded from Paessler AG's website and be printed: http://www.paessler.com/order/terms. Upon request to agb@paessler.com <mailto:agb@paessler.com> Paessler AG will provide you with a digital or written version.
I accept the agreement
I do not accept the agreement
www.paessler.com
< Back
Next >
Cancel

Setup Wizard License Agreement

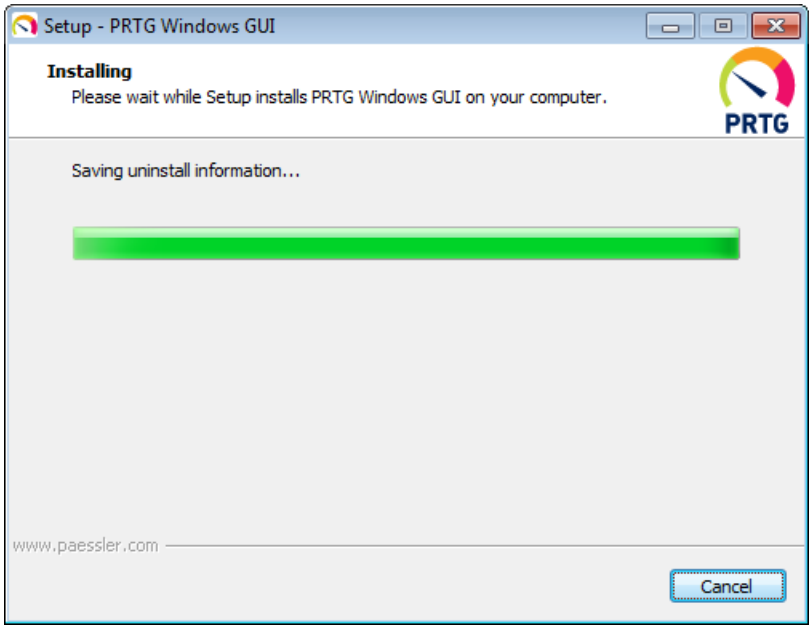
After accepting the license agreement, you can choose the folder you wish to install the software in. We recommend using the default value.

© 2011 Paessler AG


Setup - PRTG Network Monitor
Select Destination Location
Where should PRTG Network Monitor be installed?
PRTG
Setup will install PRTG Network Monitor into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\PRTG Network Monitor
Browse...
At least 228.8 MB of free disk space is required.
www.paessler.com
< Back
Next >
Cancel

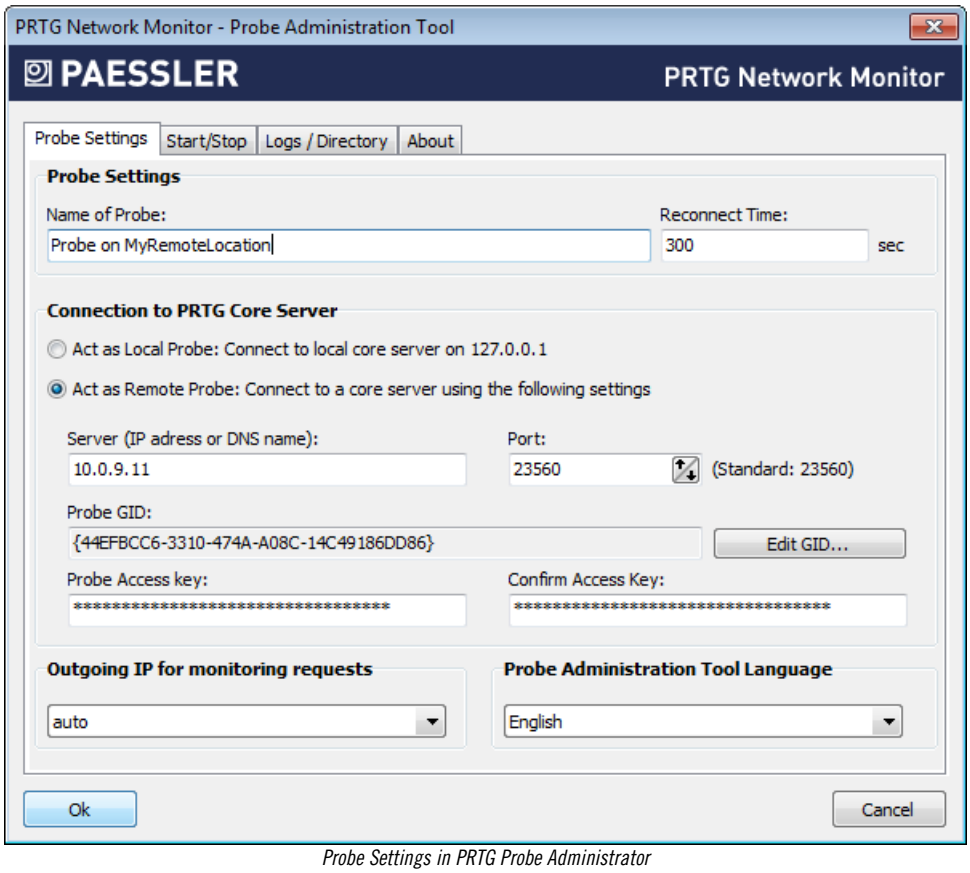
Setup Wizard Destination Location

As soon as you click **Next**, the necessary files will be copied to your disk.



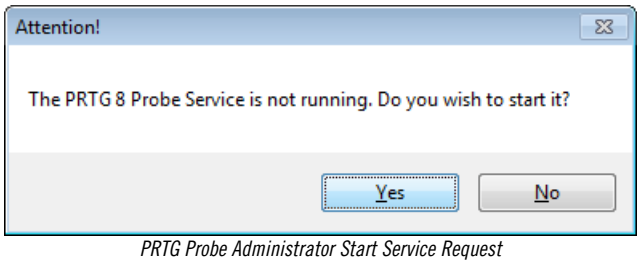
Windows GUI Setup Wizard Install

The PRTG Probe Administrator is shown. Please enter the correct settings in order to connect with your PRTG core installation. See Multiple Probes and Remote Probes 986 section for more information. Click **Ok** to continue.



Probe Settings in PRTG Probe Administrator

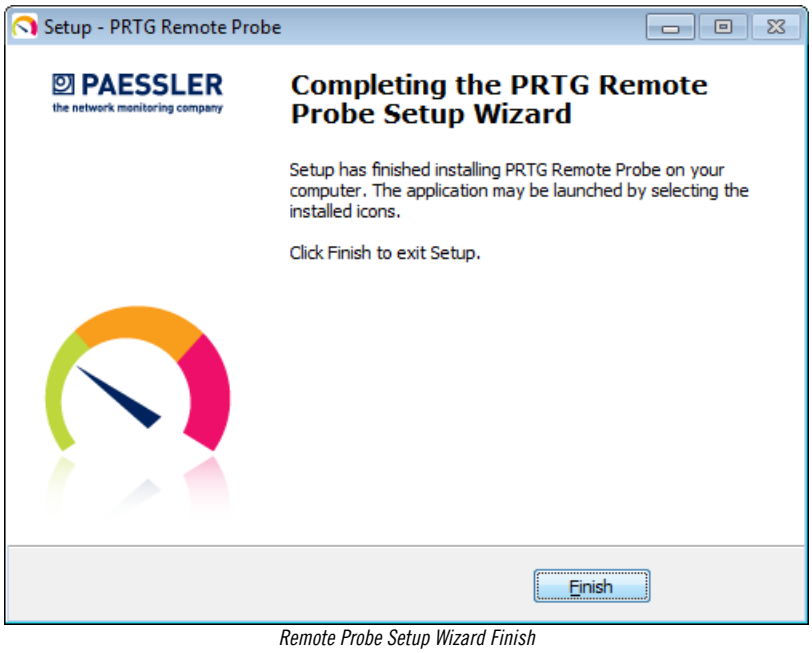
When asked if you want to start the probe service, confirm with **Yes**. The installation is completed.



PRTG Probe Administrator Start Service Request

After installation, click **Finish**.

© 2011 Paessler AG


Setup - PRTG Remote Probe
PAESSLER
the network monitoring company
Completing the PRTG Remote Probe Setup Wizard
Setup has finished installing PRTG Remote Probe on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Finish

Remote Probe Setup Wizard Finish

Your remote probe is now installed on this computer as Windows service.

More

After you click the **Finish** button, the PRTG Probe Administrator is shown, allowing you to configure connections. Please see section Remote Probe Setup 990 for more information on how to connect the remote probe with your PRTG core server installation.

3.8 Install the Windows GUI

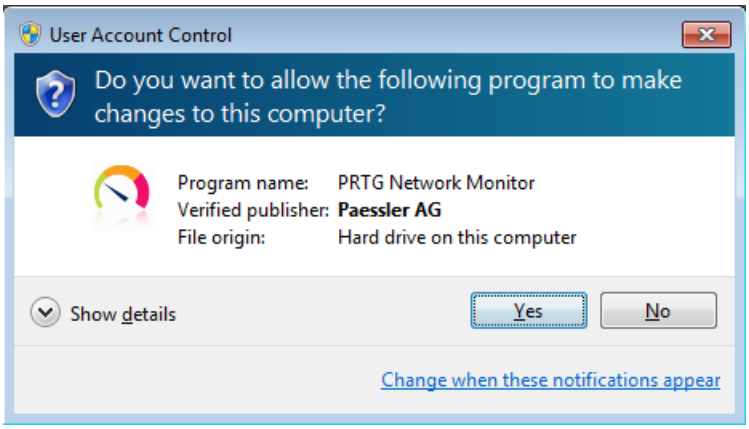
The Windows GUI is already included in a PRTG core server installation [41]. You can install additional Windows GUIs on other computers.

Download Windows GUI from the Web Interface

The Windows GUI version has to fit exactly the PRTG core server version you will connect to. In order to download your setup program to the computer you want to install it on, please connect to the Ajax [92] web interface from the computer on which you want to install the Windows GUI. In the login screen [94] of the web interface, enter login name and password and select the **Windows GUI (Download)** option. You browser will show a download dialog. Save the setup program to the local hard disk drive.

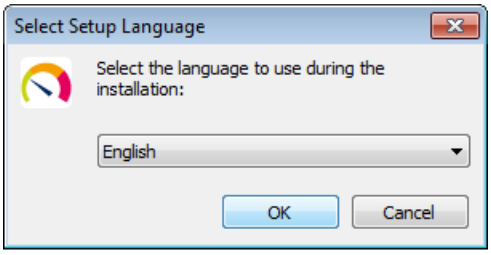
Install Windows GUI

Please execute the installation setup program you've just downloaded.


User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: PRTG Network Monitor
Verified publisher: Paessler AG
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

Windows User Account Control Confirmation Request

Confirm the question of the Windows User Account Control with **Yes** to allow the program to install. The usual software installation wizard will guide you through the installation process.



Setup Language Selection

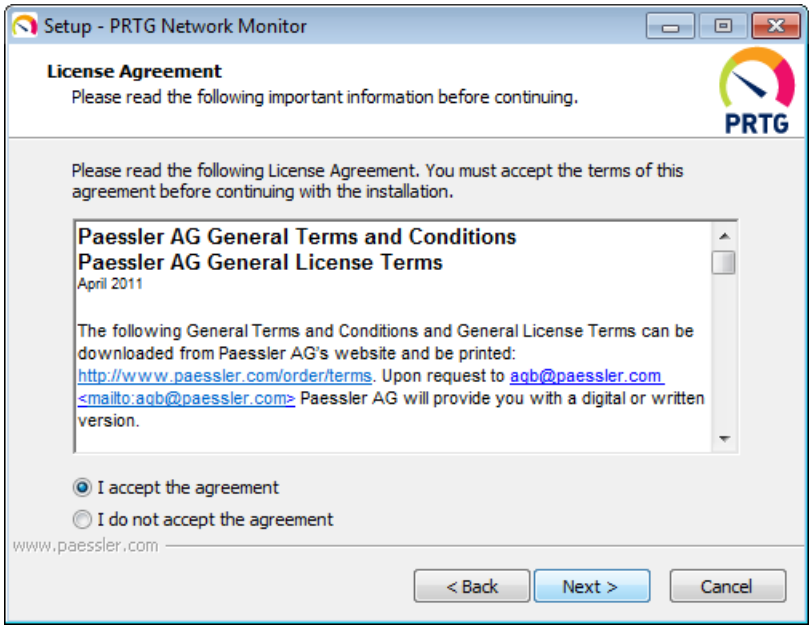
Please select a language for your product and click the **OK** button. The available language options depend on both your Windows version and the setup file.

© 2011 Paessler AG

Setup - PRTG Windows GUI
PAESSLER
the network monitoring company
Welcome to the PRTG Windows GUI Setup Wizard
This will install PRTG Network Monitor - Windows GUI on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

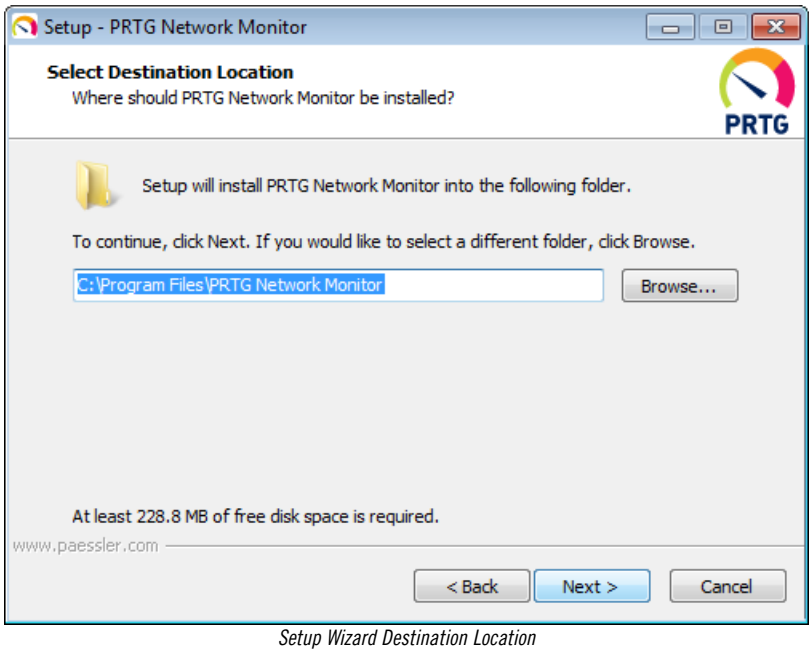
Windows GUI Setup Wizard Welcome Screen

Please click **Next** to walk through the wizard.


Setup - PRTG Network Monitor
License Agreement
Please read the following important information before continuing.
PRTG
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Paessler AG General Terms and Conditions
Paessler AG General License Terms
April 2011
The following General Terms and Conditions and General License Terms can be downloaded from Paessler AG's website and be printed: http://www.paessler.com/order/terms. Upon request to agb@paessler.com <mailto:agb@paessler.com> Paessler AG will provide you with a digital or written version.
I accept the agreement
I do not accept the agreement
www.paessler.com
< Back
Next >
Cancel

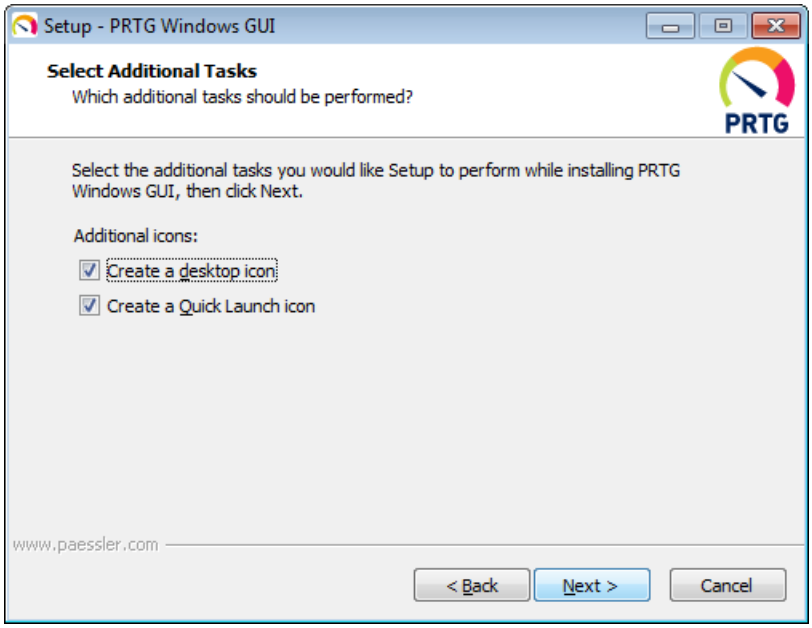
Setup Wizard License Agreement

After accepting the license agreement, you can choose the folder you wish to install the software in. We recommend using the default value.


Setup - PRTG Network Monitor
Select Destination Location
Where should PRTG Network Monitor be installed?
PRTG
Setup will install PRTG Network Monitor into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\PRTG Network Monitor
Browse...
At least 228.8 MB of free disk space is required.
www.paessler.com
< Back
Next >
Cancel

Setup Wizard Destination Location

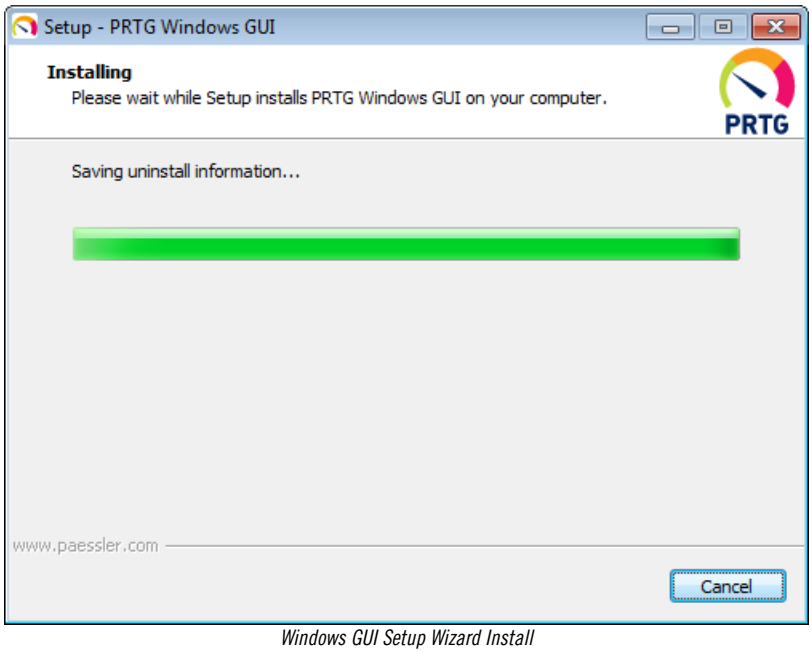
Select which icons will be created. We recommend using the default value.


Setup - PRTG Windows GUI
Select Additional Tasks
Which additional tasks should be performed?
PRTG
Select the additional tasks you would like Setup to perform while installing PRTG Windows GUI, then click Next.
Additional icons:
Create a desktop icon
Create a Quick Launch icon
www.paessler.com
< Back
Next >
Cancel

Windows GUI Setup Wizard Additional Tasks

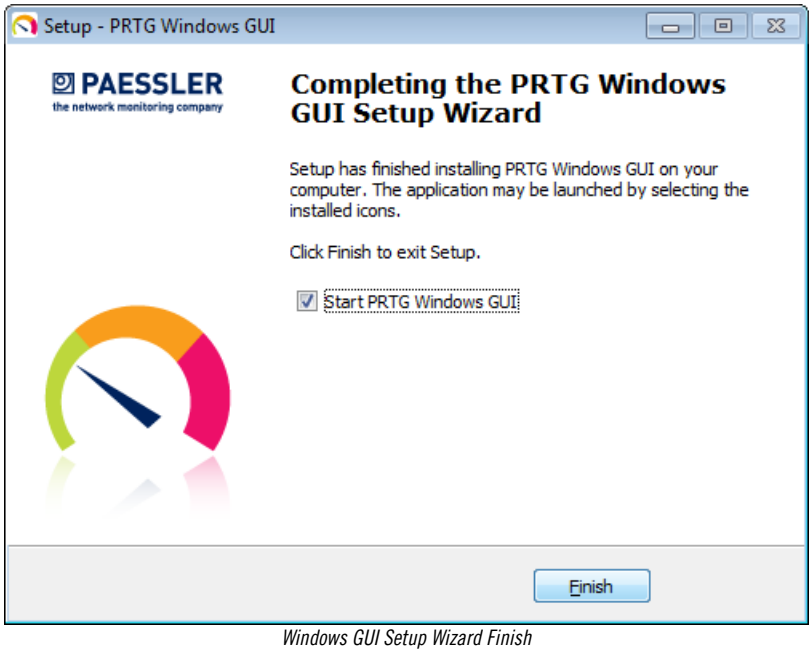
As soon as you click **Next**, the necessary files will be copied to your disk.

© 2011 Paessler AG



Windows GUI Setup Wizard Install

After installation, click **Finish** to start the Windows GUI.


Setup - PRTG Windows GUI
PAESSLER
the network monitoring company
Completing the PRTG Windows GUI Setup Wizard
Setup has finished installing PRTG Windows GUI on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Start PRTG Windows GUI
Finish

Windows GUI Setup Wizard Finish

More

Please see section Windows GUI 894 for more information on how to use this Graphical User Interface (GUI).

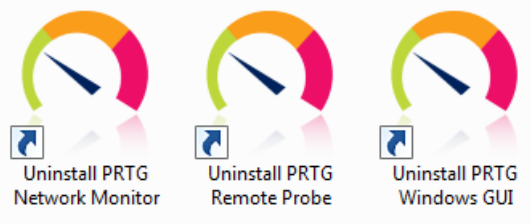
© 2011 Paessler AG

3.9 Uninstall PRTG Products

The uninstall process has six steps—regardless of if you are uninstalling an entire PRTG Network Monitor installation, a single Windows GUI installation, or a PRTG Remote Probe installation. Use the Windows uninstall routines to remove the PRTG software from your system.

Step 1

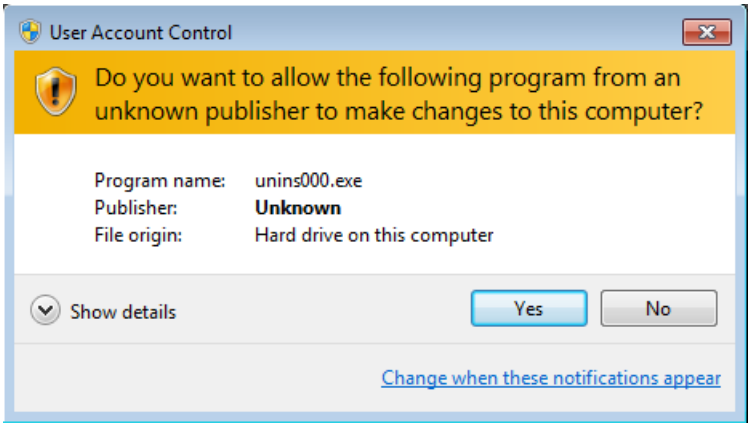
From the Windows Start Menu, select the **Uninstall PRTG Network Monitor** icon, the **Uninstall PRTG Windows GUI** icon, or the **Uninstall PRTG Remote Probe** icon, or open your Windows Control Panel and choose the respective entry in the **Programs** section. Depending on the installed products, not all uninstall programs are available.



Start Menu Icons

Step 2

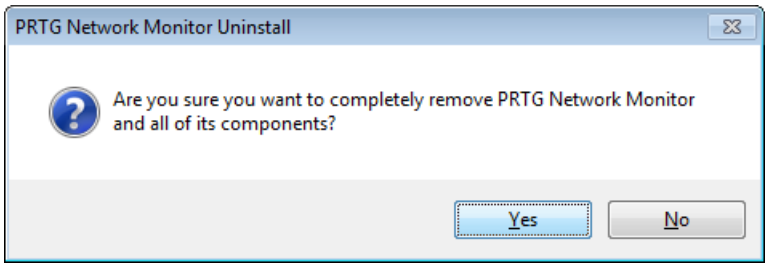
If asked, confirm the question of the Windows User Account Control with **Yes** to allow the program to uninstall. The usual software uninstall wizard will guide you through the uninstall process.


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: unins000.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

Windows User Account Control Request

Step 3

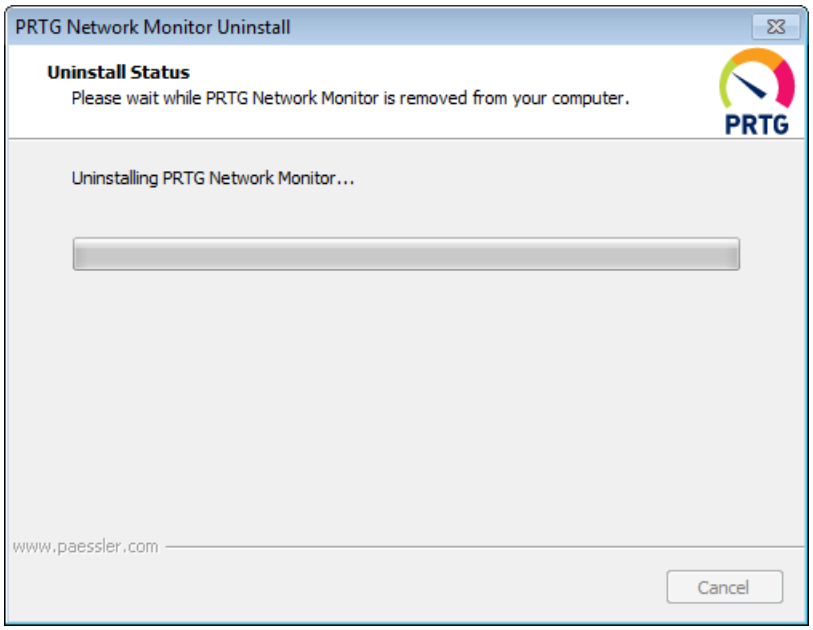
Confirm the removal of the software by clicking the **Yes** button.


PRTG Network Monitor Uninstall
Are you sure you want to completely remove PRTG Network Monitor and all of its components?
Yes
No

Uninstall PRTG Network Monitor Step 1

Step 4

Wait while the software is being removed.

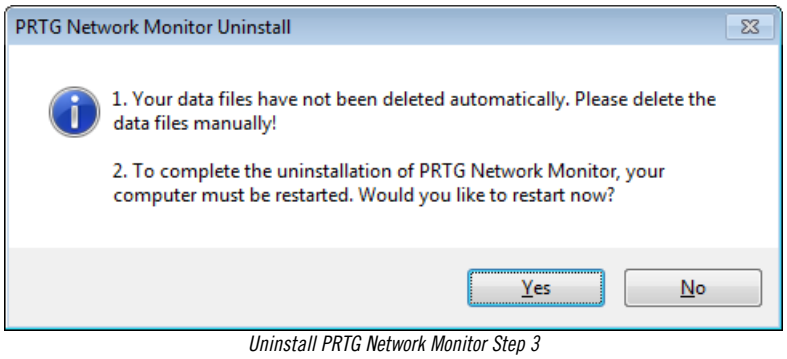


Uninstall PRTG Network Monitor Step 2

Step 5

Confirm a system restart by clicking the **Yes** button.

© 2011 Paessler AG


PRTG Network Monitor Uninstall
1. Your data files have not been deleted automatically. Please delete the data files manually!
2. To complete the uninstallation of PRTG Network Monitor, your computer must be restarted. Would you like to restart now?
Yes
No

Uninstall PRTG Network Monitor Step 3

Step 6

After system restart, the software is removed. However, there are still custom data in the PRTG program folder left. If you have uninstalled an entire PRTG Network Monitor installation or a remote probe installation, your monitoring data is still stored on the system. To completely remove all PRTG data, please delete the **PRTG Network Monitor** program folder as well as the **Paessler\PRTG Network Monitor** folder in your data path. For more information where data is stored see the **More** 71 section below.

More

Knowledge Base: How and where does PRTG store its data?

- http://www.paessler.com/knowledgebase/en/topic/463

Part IV

Understanding Basic Concepts

4 Understanding Basic Concepts

There are a number of basic concepts that lay the foundation for the functionality and ease of use of the PRTG Network Monitor. We have made using our software as easy as possible. Nevertheless, there are some basic principles we would like to explain to you. Please read this section carefully to make it easier for you to understand how best to use the software.

Understanding Basic Concepts—Topics

- Architecture 75
- Clustering 78
- Object Hierarchy 79
- Inheritance of Settings 82
- Tags 84
- Dependencies 85
- Scheduling 86
- Notifying 87
- Data Reporting 88
- User Access Rights 89

© 2011 Paessler AG

4.1 Architecture

PRTG Network Monitor consists of different parts which can be divided into three main categories: System parts, control interfaces and basic administration interfaces.

Type	Part of PRTG
System Parts	Core Server 75 This is the central part of a PRTG installation and includes data storage, web server, report engine, a notification system, and more.
	Probe(s) 76 The part of PRTG on which the actual monitoring is performed. There are local probes, remote probes, and cluster probes available. All monitoring data is forwarded to the central core server.
User Interfaces	Ajax Web Interface 92 The Ajax-based web interface is used for configuration of devices and sensors, as well as the review of monitoring results. Also system administration and user management are configured here.
	Windows GUI 894 A native Windows application as alternative to the web interface. Supports the most important features.
	iPRTG iPhone Interface 930 Monitor your network on the go with the iPhone App for PRTG.
System Administration Programs	PRTG Server Administrator 955 Used to configure basic core server settings, such as administrator login, web server IPs and port, probe connection settings, cluster mode, system language, and more.
	PRTG Probe Administrator 969 Used to configure basic probe settings such as name of the probe, IP and server connection settings, and more.

Core Server

The core server is the heart of your PRTG system and performs the following processes:

- Configuration management for object monitoring
- Management and configuration of the connected probes
- Cluster management
- Database for monitoring results
- Notification management including a mail server for email delivery
- Report generator and scheduler
- User account management
- Data purging (culling data that is older than 365 days, for example)
- Web server and API server

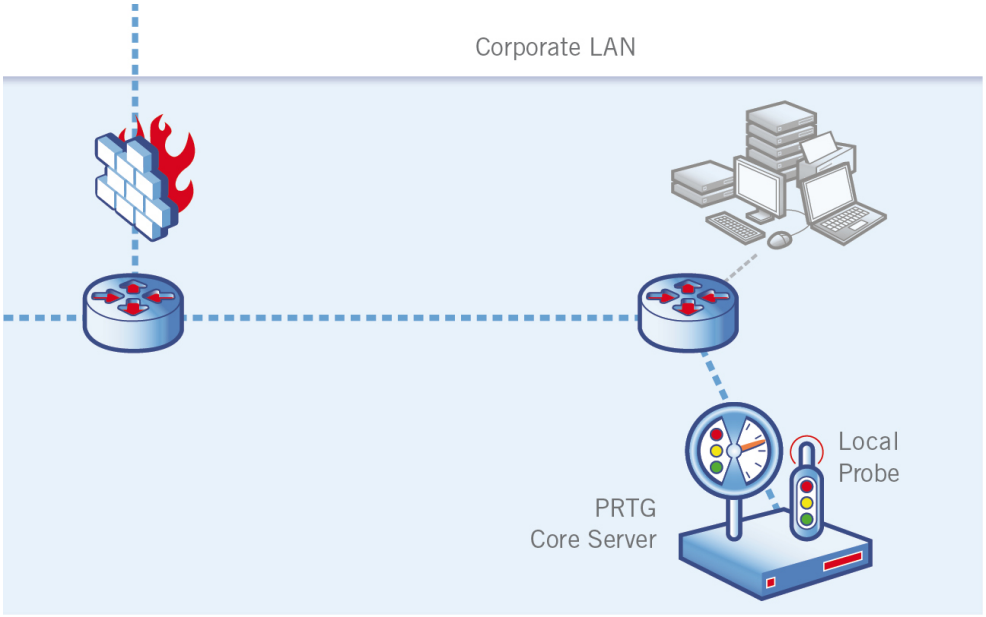
In a cluster, the current master node is responsible for all of these tasks.

The built-in, fast and secure web server (no IIS or Apache is required) supports HTTP as well as secure HTTPS (via SSL). It serves the web interface when accessed with a browser and also answers PRTG Application Programming Interface (API) calls (e.g. for user scripts, or the Windows GUI).

Note: Core server and probe(s) are configured as Windows services which are permanently run by the Windows system without the requirement for a logged-in user.

Probe(s)

On a probe, the sensors created on a device perform the actual monitoring. The probe receives its configuration from the core server, runs the monitoring processes and delivers monitoring results back to the core server. On every system running a PRTG core server, there is always a local probe running with it.



PRTG Core Server and Local Probe Monitoring a Local Area Network

The actual monitoring is performed by PRTG probe processes which run on one or more computers. During installation the so-called **Local Probe** is automatically created by the system. In a single-probe installation—which is the default setup—all monitoring is performed by the local probe.

The PRTG core server inside the corporate LAN (bottom right) is able to monitor services and servers in the entire Local Area Network (LAN). *Note:* Core server and probe(s) are configured as Windows services which are permanently run by the Windows system without the requirement for a logged-in user.

In a cluster setup 78, a cluster probe runs on all nodes. There is an additional so-called **Cluster Probe**. All devices created on it are monitored by all nodes in the cluster, so data from different perspectives is available and monitoring for these devices always continues, also if one of the nodes fails.

© 2011 Paessler AG

PRTG automatically monitors system health of its own core server and of each probe in order to discover overloading situations that may distort monitoring results. To monitor the system status of the probe computer, PRTG automatically creates a few sensors. These include **Core/Probe Health**, **Cluster Probe Health**, **Disk Free**, and a bandwidth sensor for all installed network cards. We recommend keeping these sensors, but you can optionally remove all except the **Health** sensors. They measure various internal system parameters of the probe system hardware and the probe's internal processes and then computes a resulting value. Frequent or repeated values below 100% should be investigated. Please check the sensor's channels 104 for details.

Additional so-called **Remote Probes** can be created by the user in order to achieve monitoring of multiple locations, or for several other scenarios. They are using SSL-secured connections to the core and allow to securely monitor services and systems inside remote networks which are not openly accessible, or secured by firewalls. For more information please see **Remote Probes and Multiple Probes** 986 section. For a video on this please see **More** 155 section below.

More

Video Tutorial: There is a video available on the Paessler video tutorials page.

- http://www.paessler.com/support/video_tutorials

4.2 Clustering

A PRTG Cluster consists of two or more installations of PRTG 41 that work together to form a high availability monitoring system. The objective is to reach true 100% uptime for the monitoring tool. Using clustering 53, the uptime will no longer be degraded by failing connections because of an Internet outage at a PRTG server's location, failing hardware, or because of downtime due to a software upgrade for the operating system or PRTG itself.

How a PRTG Cluster Works

A PRTG cluster consists of one **Primary Master Node** and one or more **Failover Nodes**. Each node is simply a full installation of PRTG which could perform the whole monitoring and alerting on its own. Nodes are connected to each other using two TCP/IP connections. They communicate in both directions and a single node only needs to connect to one other node to integrate into the cluster.

During normal operation the **Primary Master** is used to configure devices and sensors (using the web interface 92 or Windows GUI 894). The master automatically distributes the configuration to all other nodes in real time. All nodes are permanently monitoring the network according to this common configuration and each node stores its results into its own database. This way also the storage of monitoring results is distributed among the cluster (the downside of this concept is that monitoring traffic and load on the network is multiplied by the number of cluster nodes, but this should not be a problem for most usage scenarios). The user can review the monitoring results by logging into the web interface of any of the cluster nodes in read only mode. As the monitoring configuration is centrally managed, it can only be changed on the master node, though.

All devices created on the **Cluster Probe** are monitored by all nodes in the cluster, so data from different perspective is available and monitoring for these devices always continues, also if one of the nodes fails. In case the **Primary Master** fails, one of the **Failover Nodes** takes over the master role and controls the cluster until the master node is back. This ensures a fail-safe monitoring with gapless data.

If downtimes or threshold breaches are discovered by one or more nodes only one installation, either the Primary Master or the Failover Master, will send out notifications (via email, SMS text message, etc.). So, the administrator will not be flooded with notifications from all cluster nodes in the event of failures.

More

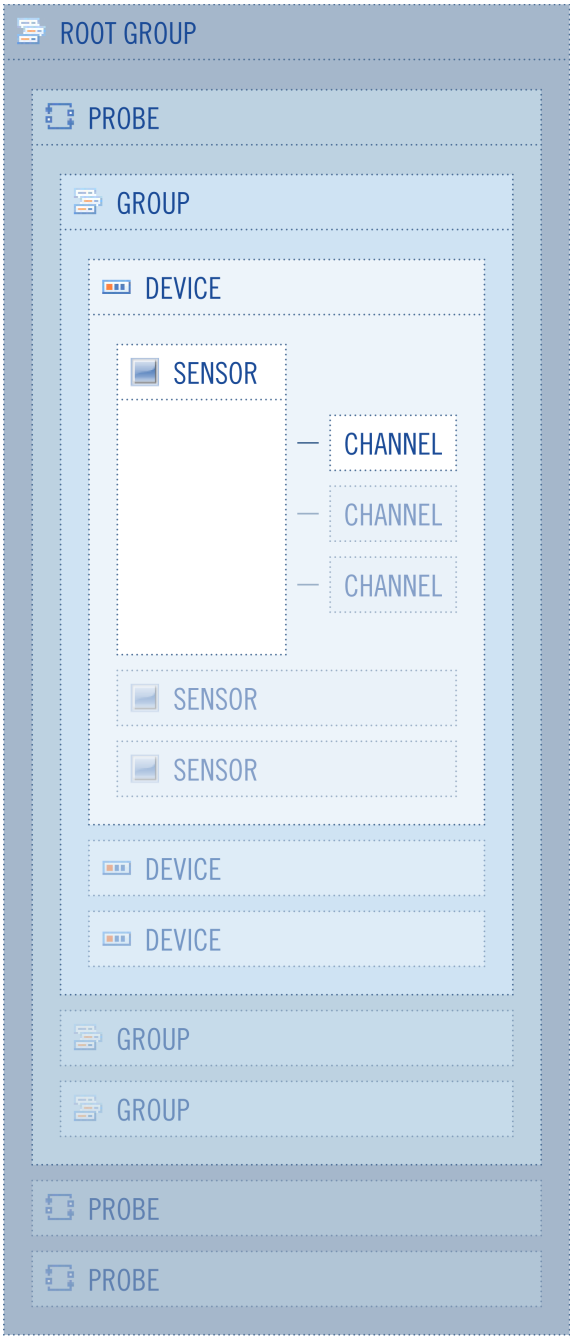
Knowledge Base: What's the Clustering Feature in PRTG 8?

- http://www.paessler.com/knowledgebase/en/topic/6403

© 2011 Paessler AG

4.3 Object Hierarchy

All objects in a PRTG monitoring configuration are arranged in a tree-like hierarchy to create an easy to navigate list and to give the user the possibility to arrange them in groups that monitor similar devices, services, or same locations. The hierarchical order described is also used to define common settings for larger groups of objects, for example settings of the **Root** group apply by default to all other objects below it (see section Inheritance of Settings 82).



Object Hierarchy in PRTG

Root Group

The **Root** group is the topmost instance in PRTG. It contains all other objects in your setup. Using the inheritance 82 mechanism, we recommend adjusting the default settings for the Root group 166 in order for all other objects to inherit them. This makes configuration easier later on.

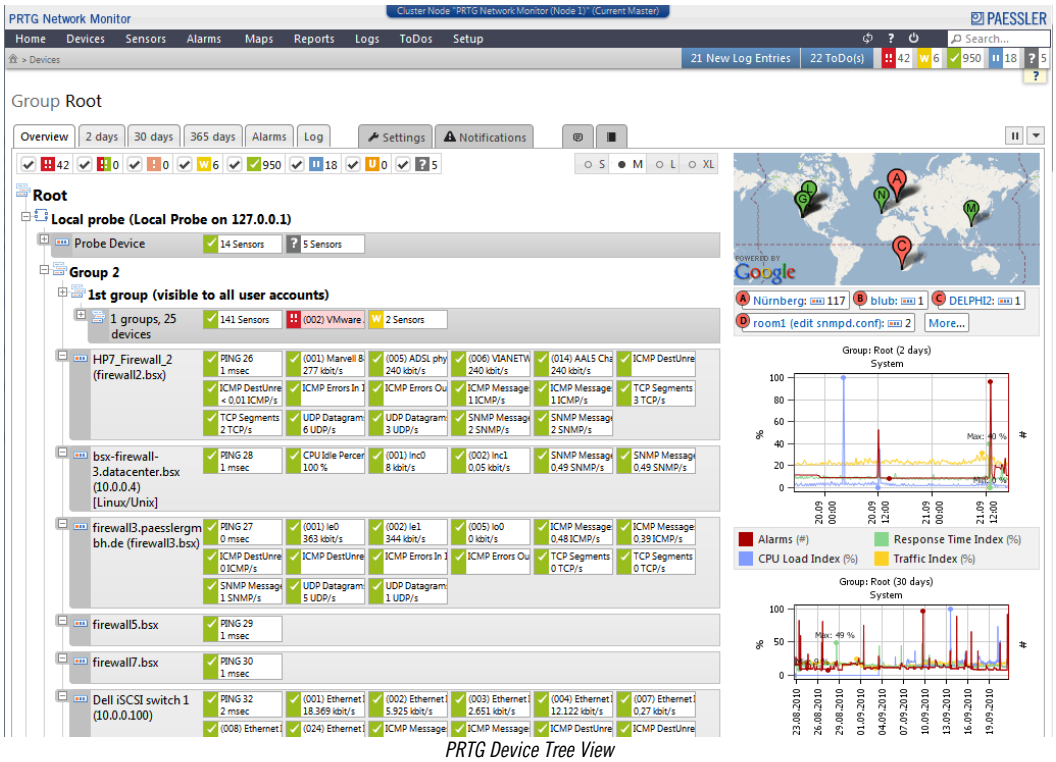
Probe

Each group (except the **Root** group) is part of a **Probe**. This is the platform on which the monitoring takes place. All objects configured below a probe will be monitored via that probe. Every PRTG core installation automatically installs a **Local Probe** service. You can add additional probes and remote probes to your configuration to include remote devices from outside your network into the monitoring (see section **Multiple Probes and Remote Probes** 986). In a cluster, there is an additional **Cluster Probe** running on all nodes. Devices on the cluster probe are monitored by all nodes of the cluster, so data from different perspective is available and monitoring for these devices always continues, also if one of the nodes fails.

Group

On each probe, there are one or more **Groups**, which serve merely structural purposes. Use groups to arrange similar objects in order to inherit same settings to them. To a group, you add the devices. You can arrange your devices in different nested groups to reflect the structure of your network.

Find below a sample configuration: A device tree with local probe, several groups, devices and their sensors.



PRTG Device Tree View

© 2011 Paessler AG

Device

To each probe or group, you can add **Devices** that you want to monitor. Each device in your PRTG configuration represents a real hardware device in your network. These can be, for example:

- Web or file server
- Client computer (Windows, Linux, or Mac OS)
- Router or network switch
- Almost every device in your network that has its own IP address

PRTG additionally adds a so called **Probe Device** to the local probe. This is an internal system device. It has access to the computer on which the probe is running on and monitors its health parameters with several sensors running on it.

Sensor

On each device you can create a number of **Sensors.** Every sensor monitors one single aspect of a device. This can be, for example:

- One network service like SMTP, FTP, HTTP, etc.
- One network switch port's traffic
- CPU load of a device
- Memory load of a device
- Traffic of one network card
- One NetFlow device
- etc.

Channel

Every sensor has a number of **Channels** through which it receives the different data streams. The available channels depend on the type of sensor. One sensor channel can contain, for example:

- **Downtime** for a device
- **Traffic in** of a bandwidth device (e.g. a router)
- **Traffic out** of a bandwidth device (e.g. a router)
- **Traffic sum** of a bandwidth device (e.g. a router)
- **WWW traffic** of a NetFlow device
- **Mail traffic** of a NetFlow device
- **Other traffic** of a NetFlow device
- **CPU Load** of a device
- **Loading time** of a web page
- **Download Bandwidth** of a web page
- **Time to first byte** of a web page
- **Response time** of a Ping request to a device
- **Response time** of a Remote Desktop service
- etc.

© 2011 Paessler AG

4.4 Inheritance of Settings

The hierarchical tree 79 is not only used to group sensors for organizational reasons, there is also an important aspect involved that we call inheritance. To ensure administration is quick and easy—especially for large monitoring setups—certain settings are inherited from the overlying level. For example, you can change the monitoring interval for all sensors by editing the interval setting of the topmost **Root** group (unless no other setting is defined below).

Settings are Inherited to Child Objects

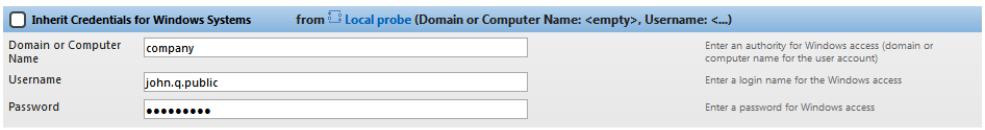
You can override this inheritance on any level of the hierarchy by setting a different value for a specific probe, group, device, or sensor. All objects below will inherit these new settings; not the ones from levels above.

Settings that are inherited among all objects include:

- Monitoring interval
- Notification triggers
- Authentication settings for several systems
- Compatibility settings (for certain types of sensors)
- Channel and unit configuration
- User access rights
- Tags 84
- Paused status: If an object is paused by the user, or a schedule, all sensors on it are paused as well
- etc.

There is one exception for devices and sensors: The **IP address** or **DNS name** of a device and compatibility settings are always inherited by sensors and can not be changed on sensor level.

The actual overriding of the parent's settings takes place in an object's settings: Remove the check mark symbol at the beginning of the respective line **Inherit Abc from Xyz**. As an example, the screenshot below shows Windows systems credentials settings after removing the check mark symbol.


Inherit Credentials for Windows Systems
from Local probe (Domain or Computer Name: <empty>, Username: <...)
Domain or Computer Name
company
Enter an authority for Windows access (domain or computer name for the user account)
Username
john.q.public
Enter a login name for the Windows access
Password
Enter a password for Windows access

Credentials for Windows Systems

Default Values Set in Root Group

For all settings (except passwords) PRTG already includes a set of default values so you can get started with the software immediately. For example, the following settings will be inherited by all sensors from the **Root** group:

- Default monitoring interval of one minute
- SNMP version 1 with community string set to **public** (default values for most devices)
- Dependency type **Use parent**
- etc.

© 2011 Paessler AG

You may need to change some of the default entries as you become used to the interface. However, these settings should initially suffice for most situations.

Before sensor setup, please review the Root group's settings and set the default values to suit your setup, including necessary credentials for all kinds of systems in your network you want to monitor (Windows, Linux, virtual servers, etc.). See section Root Group Settings 166 for more details.

4.5 Tags

For every object in your PRTG setup, you can not only name objects, but also define tags in an object's settings 111 to additionally mark an object as a member of certain categories. Although there are tags predefined when adding objects 156 you are totally free in the way you add tags. For example, you could mark all of the bandwidth sensors that are especially important for you with a tag *bandwidth_important*. Later, you can view lists of objects with certain tags, or choose sensors by tag when creating reports 827. A clever arrangement of tags can save you a lot of time later. *Note:* You can change tags for several objects at a time using the multi-edit 813 function.

Tags Are Inherited

The tags in an object's settings are automatically inherited 82 to all other objects further down in the hierarchy. So, for example, a device with the tag *myExampleTag* will automatically and invisibly inherit this tag to all sensors created on it. This will not be visible in the sensor's tag settings, but the sensors will appear in the list whenever you search for *myExampleTag*. This is useful, for example, when adding sensors by tag in reports 827 settings. This way, to configure your setup for fetching all sensors on a device by tag, you do not have to tag every single sensor, but it's enough to tag the device. Inheritance for tags cannot be disabled.

© 2011 Paessler AG

4.6 Dependencies

Using dependencies you can pause sensor monitoring based on the status of another sensor in order to avoid false alarms and incorrect downtime recording. A dependency stops the monitoring of one sensor or a set of sensors as soon as a specific sensor is not in an **Up** status. This means, for example, you can stop monitoring remote network services when the corresponding firewall is down due to connection problems.

When using the auto-discovery 145 function, the **Ping** sensor on a device is by default set as the master object for this device. This means that monitoring for the entire device is paused if the Ping sensor is in a **Down** status. Usually, it does not make sense to monitor other aspects of a device with other sensors, while the **Ping** sensor indicates that the device is not even reachable.

For more information about the dependency settings, please see the settings of the respective object 111 you want to set a dependency for.

Related Topics

- **Show Dependencies** 821

4.7 Scheduling

Using schedules, monitoring of an object can be paused 123 for a certain time, for example, Sundays between 4 and 8 a.m. A paused sensor will not collect monitoring data, will not change its status, and will not trigger any notifications 87. With schedules you can limit the monitoring time automatically. You can also pause monitoring for planned system maintenance time spans to avoid false alarms. You can apply different schedules to every object. They are also used for reports and notifications.

Schedules are user account specific. To change the default pre-defined schedules or to add your own schedule, please see **Account Settings—Schedules** 868 section.

© 2011 Paessler AG

4.8 Notifying

PRTG keeps the administrator or others informed about the current status of the network. There are several methods how the administrator can stay up to date.

Notifications

This is the most powerful information tool. Whenever PRTG discovers downtime, an overloaded system, threshold breach, or similar situations, it can send a notification. Notifications use various methods by which you can be notified (e.g. email, SMS, pager message and others). After creating notifications in the system settings, you can select them on the setting pages for a group, a device, and a sensor. See **Notifications** 825 section for more details.

Limits

In a sensor channel's settings 792 you can set limits to change the status of the sensor when certain limits are breached. This way, you can set e.g. a traffic sensor, which is typically never in a error status, to **Down** status whenever bandwidth values are measured that you consider critical. This sensor will then show up in the alarms list.

Alarms

The alarm list shows all sensors that are currently in a **Down**, **Down (Partial)**, **Warning**, or **Unusual** status. This is useful to keep track of all irregularities in your network. In the table list, you can re-sort the items by clicking on the column's header items. See **Alarms** 113 section for more details.

Logs

In the Log list, the log file with all monitoring events is shown. In a typical setup, a huge amount of data is produced here. As the activity of every single object is minuted, you can use this data to check exactly if your setup works as expected. See **Logs** 115 section for more information.

ToDos

The ToDos list shows items with important system information or action steps to take for the administrator. Every ToDo should be viewed and acknowledged. Per default, an email is sent to the administrator for every new ToDo that is created by the system. See **ToDos** 117 section for more information.

© 2011 Paessler AG

4.9 Data Reporting

With reports you can analyze and review monitoring data for specific time spans. There are several ways to create data reports in PRTG.

View Historic Data

To get a report for a single sensor, there is a function included to review historic data in PRTG. It allows you to generate reports and charts for a single sensor's data. See Historic Data Reports 107 section for more information.

Generate Reports

You can use the sophisticated reports machine included in PRTG to create exhaustive reports for all monitoring data. See Reports 827 section for more information.

Exporting Data Using the API

You can also export all monitoring raw data to XML or CSV files and generate your own reports using any third party software. See Using the PRTG API (Application Programming Interface) 979 section for more information.

Making Data Available

You can make monitoring data available to others using a special read only user (see User Access Rights 89 section), or you can create public or semi-public HTML pages with monitoring data using the Maps feature. See Maps 842 section for more information.

Bill Customers

You can also create custom billing reports based on PRTG's monitoring data, using the open source Billing Tool for PRTG. For details and download, please see Downloads 890 section.

© 2011 Paessler AG

4.10 User Access Rights

The default administrator can use the PRTG installation as the only user or can create an unlimited number of users. Users are organized using an unlimited number of groups (which also control their security settings). All access rights are defined on group level in the settings of each object in your PRTG device tree.

There are administrator users, read/write users, and read only users. With these tools, you can create a rights management that allows you to specify exactly what users will be able to see and edit. All the security settings as well as further rights management are conducted via the user groups. This means that group membership controls what a user may do and which objects he/she sees when logged in. The actual rights for each object can be defined in an object's settings. There, you can define different rights for each user group. Again, these settings are inherited.

For more information about defining rights, please see the following sections:

- System Administration—User Accounts 884
- System Administration—User Groups 887

You can define access rights for each user group in the settings of a probe, group, device, or sensor. For more information, please see Object Settings 111 section.

Part V

Ajax Web Interface—Basic Procedures

5 Ajax Web Interface—Basic Procedures

The Ajax-based web interface is your access to PRTG. It is used to configure devices and sensors, and to set up notifications, as well as review monitoring results and create reports. This web interface is highly interactive and uses Asynchronous Java Script and XML (AJAX) to deliver a powerful and easy-to-use user experience. While the user is logged in 93, the data on the screen is permanently refreshed (via Ajax calls) so it always shows the current monitoring results (refresh interval and method can be set 884 by the user).

The following sections introduce the features and concepts of the Ajax Graphical User Interface (GUI).

Ajax Web Interface—Basic Procedures—Topics

- Login 93
- General Layout 97
- Sensor States 102
- Review Monitoring Data 104
- Historic Data Reports 107
- Object Settings 111
- Alarms 113
- Logs 115
- ToDos 117
- Working with Table Lists 119
- Object Selector 120
- Priority and Favorites 122
- Pause 123
- Context Menus 124
- Main Menu Structure 133

Other Ajax Web Interface Sections

- Ajax Web Interface—Device and Sensor Setup 144
- Ajax Web Interface—Advanced Procedures 806

Related Topics

- Windows GUI 894
- Other User Interfaces 926

© 2011 Paessler AG

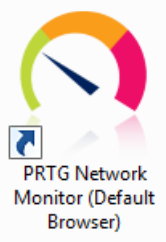
5.1 Login

Once the PRTG core server is installed 41, you can login to the web interface as administrator using the IP address, login name and password defined during setup 41. If configured respectively, you can log into PRTG from any computer within your network.

You can look up and change PRTG's web server settings at any time using the PRTG Server Administrator 955 Windows application on the system PRTG core server is installed on.

Loading the Web Interface

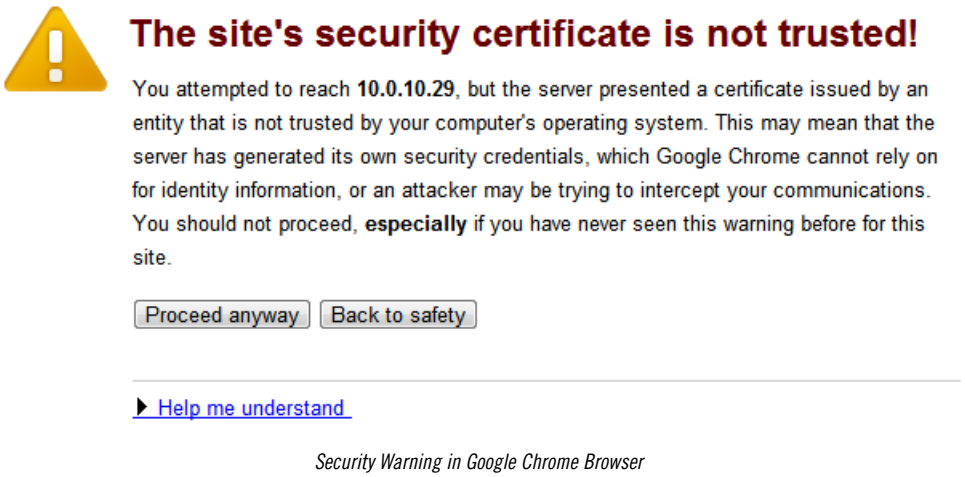
In a web browser window, please enter the IP address or URL of the system PRTG is installed on. When using a cluster, please connect to the primary master node. You can also double click on the **PRTG Network Monitor** icon on the desktop of the system PRTG is installed on.



Desktop Icon

Confirm Certificate for Https Connection

In a standard setup, the connection to the web interface is SSL-encrypted, using a certificate that is automatically installed with PRTG. Although the connection is securely encrypted, it is not a "trusted" certificate issued by a known entity. That's why usually your browser will show a certificate warning that may look like the following:


The site's security certificate is not trusted!
You attempted to reach 10.0.10.29, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, especially if you have never seen this warning before for this site.
Proceed anyway
Back to safety
Help me understand

Security Warning in Google Chrome Browser

Every browser shows this warning in a different layout. The certificate that comes with PRTG is not insecure, but simply not signed by a valid authority. In order to proceed to the login screen, please confirm the claimed "security risk". The steps to take are similar for every browser, yet different in detail.

Example

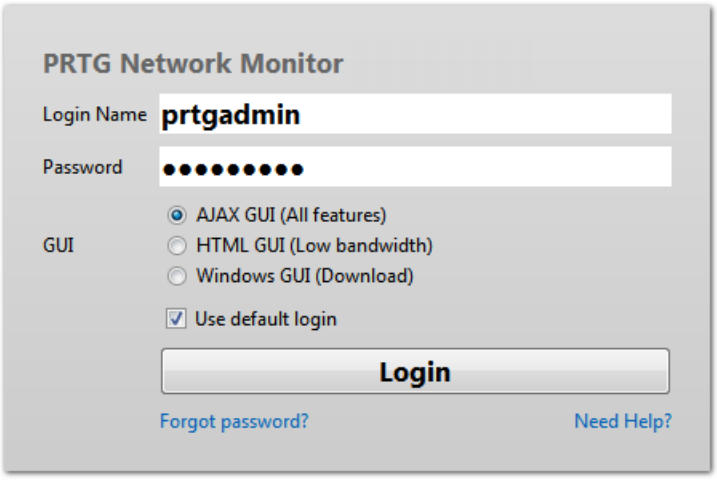
As an example how to confirm an unknown certificate, find below a description for the most common web browsers:

- In **Google Chrome 5**, click on **Proceed anyway** every time you call the web interface.
- In **Mozilla Firefox 3**, click on **I Understand the Risks**, **Add Exception...**, **Get Certificate**; leave the check mark for **Permanently store this exception**; and finally click on **Confirm Security Exception**. You only have to go through this procedure once for every Firefox browser and PRTG core server.
- In **Internet Explorer 8** or **9**, click on **Continue to this website (not recommended)** every time you call the web interface. We recommend to not use Internet Explorer 8 or earlier.

For more information on secure browser connections, please see the More 96 section below.

Login Screen

After loading the web interface, the login screen is shown:



PRTG Login Screen

© 2011 Paessler AG

There are two possibilities for login: You can enter credentials for the default administrator account, or you can login as a (restricted) PRTG user, or another administrator. When logging in for the first time or when using PRTG as a single user, you will usually use an administrator account. With these credentials, you can use all functionalities of the web interface. The administrator can create additional users 884 with administrator rights or with more restricted privileges.

First Time Login as Administrator

When logging in for the first time, enter the administrator login name and password as defined during setup (you can look up and change these in the PRTG Server Administrator 963 Windows application). Default login name and password are both **prtgadmin**. If you have not changed them, usually the option **Use default login** appears above the **Login** button. Set a check mark to fill in the default credentials automatically.

Login as PRTG User

If you have received user credentials from your administrator, please enter them here to login. Also, when using other administrator credentials, please enter them here.

Choose GUI version

Depending on the used browser, different Graphical User Interface (GUI) options are shown:

- **AJAX GUI (All features)**: The standard interface. We recommend using it whenever possible. It offers full functionality. Use Google Chrome or Mozilla Firefox for best performance. In some browsers, the Ajax option is not shown (e.g. not in IE 7 and earlier).

  Although you can login using Internet Explorer 8 or later, this interface is *not* fully compatible with Internet Explorer! When using IE 8, please set the security level at least to **Default level Medium-high** and make sure you do not use the **Compatibility View**! For detailed information, please see **More** 96 section below.

- **HTML GUI (Low bandwidth)**: The HTML GUI (Low bandwidth) 927 interface is optimized for slow network connections. It only offers read-only functionality and comes with less scripting. It is also a fallback solution when using a browser that is not supported by the Ajax interface (e.g. when using IE7 and earlier).

- **Windows GUI (Download)**: Option to download the native Windows interface to the desktop. It has to be installed 894 on the client computer before use. The Windows GUI 894 provides full functionality; however, for some functions the Ajax GUI is opened. *Note:* Also when downloading the Windows GUI, login name and password are required!

Note: Only Google Chrome and Mozilla Firefox are fully compatible with the Ajax GUI. For more information about Internet Explorer support, please see **More** 96 section below.

Click on the **Login** button to proceed to the PRTG web interface.

More

Knowledge Base: Why don't I get an SSL connection to the PRTG web interface?
- http://www.paessler.com/knowledgebase/en/topic/11813

Knowledge Base: How can I establish a secure web interface connection to PRTG?
- http://www.paessler.com/knowledgebase/en/topic/273

Knowledge Base: How can I use a trusted SSL certificate with the PRTG web interface?
- http://www.paessler.com/knowledgebase/en/topic/283

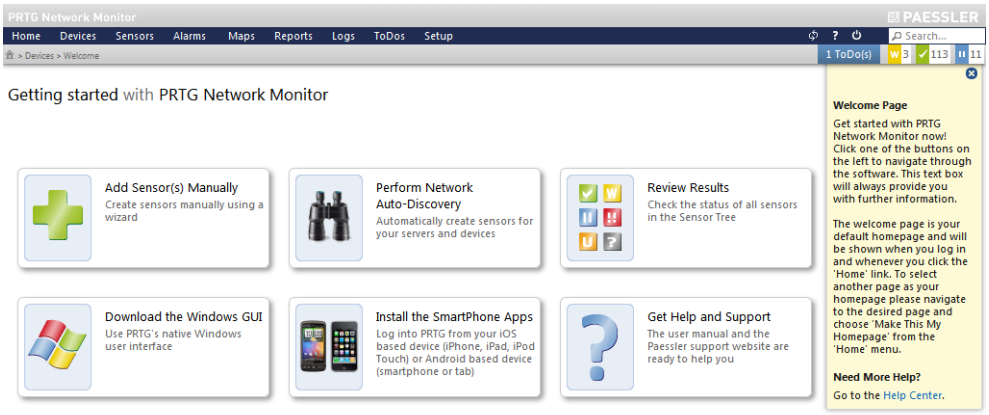
Knowledge Base: Why are Internet Explorer IE6 and IE7 not supported by PRTG's Ajax Interface?
- http://www.paessler.com/knowledgebase/en/topic/7633

Knowledge Base: How can I access the AJAX web interface of PRTG 8 with Internet Explorer 8?
- http://www.paessler.com/knowledgebase/en/topic/9483

© 2011 Paessler AG

5.2 General Layout

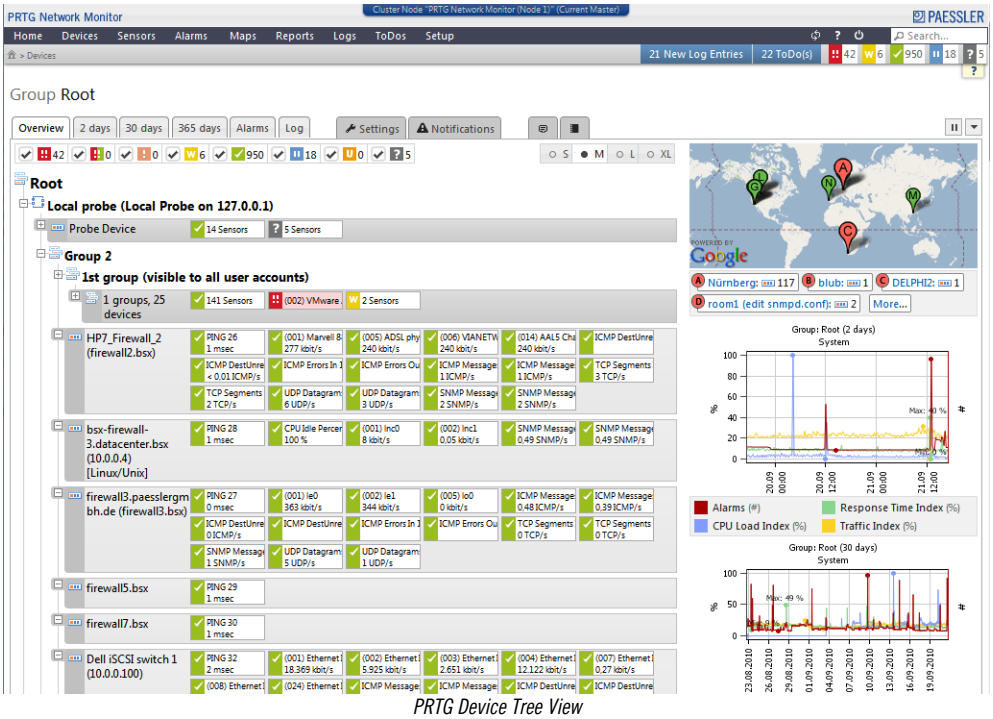
After logging into the web interface, you will see PRTG's welcome page as default. This page helps you to add sensors manually, perform an automatic network search, review results, download the Windows-GUI or iPhone application, and get further help and support.


PRTG Network Monitor
PAESSLER
Home Devices Sensors Alarms Maps Reports Logs ToDos Setup
Getting started with PRTG Network Monitor
Add Sensor(s) Manually
Create sensors manually using a wizard
Perform Network Auto-Discovery
Automatically create sensors for your servers and devices
Review Results
Check the status of all sensors in the Sensor Tree
Download the Windows GUI
Use PRTG's native Windows user interface
Install the SmartPhone Apps
Log into PRTG from your iOS based device (iPhone, iPad, iPod Touch) or Android based device (smartphone or tab)
Get Help and Support
The user manual and the Paessler support website are ready to help you
Welcome Page
Get started with PRTG Network Monitor now! Click one of the buttons on the left to navigate through the software. This text box will always provide you with further information.
The welcome page is your default homepage and will be shown when you log in and whenever you click the 'Home' link. To select another page as your homepage please navigate to the desired page and choose 'Make This My Homepage' from the 'Home' menu.
Need More Help?
Go to the Help Center.

Welcome Screen

Tree View Layout

Click on the **Review Results** option to display the tree-like device view which will be a starting point for everyday use.



PRTG Device Tree View

From top to bottom, the main layout consists of:

- The global header area 98 with the main menu at the top, the global status bar, and a quick search box.
- The page header bar 99 with the page heading containing the name of the current object, the tabs bar which leads to the content of the current object, and the object's status bar.
- The page content 100 with information about the current object and all other objects underneath in the tree hierarchy.

Simply click on an object to see more details about it. In the page heading of the page header bar 99 you always see which object you're looking at.

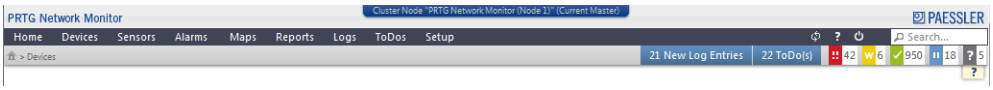
When you navigate through PRTG's web interface you will always use one of the following five navigational paths:

- The main menu provides access to all important aspects of the software.
- The quick search is often the fastest way to navigate to an object.
- Using the page's tabs, you can switch between various sub-pages for an object.
- Many objects offer a context menu that will pop up when you right-click them.
- Many objects offer a quick-info menu that will pop up when hovering an object
- And, finally, you are able to drill down into the object hierarchy of probes, groups, devices, and sensors in the object tree by merely clicking an sub-object of the currently displayed object (for example, a sensor on the device page).

These six navigation paths put PRTG's complete functionality at your fingertips. Quite likely you are already familiar with these techniques from many other websites and web-based user interfaces.

In the following, the different areas of the web interface are described.

Global Header Area



PRTG's Cluster Info, Main Menu, and Global Status Bar

The header area of the web interface is both base for the most important information of your installation and starting point for all actions. You can view the global status and navigate through the web interface using the main menu.

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

The global header area consists of the following parts:

- **Blue Cluster Information Bar**
  This element is only visible when running PRTG in a cluster. It shows the name of the node you are logged in and displays whether this is a master or a failover node. Click the bar to show the **Cluster Status** 888. In a failover node, you can review all data, but changes in the settings will not be saved. In order to change settings, please log into the master node of your cluster.

© 2011 Paessler AG

- **Grey Main Menu Bar**
  Navigating through the web interface is performed using the main menu. Please take a few minutes to familiarize yourself with all menu items and sub-items. A detailed description can be found in the Main Menu Structure 133 section.

- **Icons Refresh, Help Center, Logout**
  With the icons on the right you can reload the current page, open the help center or log the current user out.

- **'Breadcrumbs'**
  Below the main menu, there is always a path shown, leading to the homepage. Use it to go back to where you came from. It can also help you to orient yourself in case you get lost.

- **White Search Box**
  To search for any monitoring object, simply enter the name, part of the name, an IP address, a DNS name or a tag in the search box on the right and hit the enter key. A web page with all items that fit the search term will be returned—even displaying online help articles.

- **Yellow Help Box**
  A context sensitive help text for every page is displayed in the yellow help box on the right. Click on the **x** symbol to close and on the question mark **?** symbol to open it.

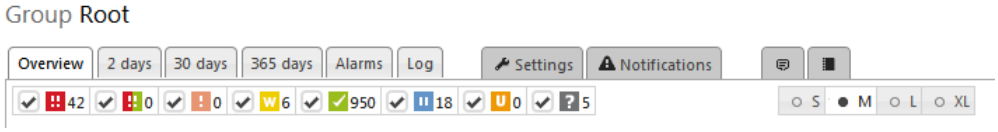
- **Buttons New Log Entries, ToDo(s)**
  These fields show the number of new log entries since last user login and the number of ToDo(s) that wait to be acknowledged. Click on the respective entry to view the Logs 115 or ToDos 117.

- **Global Sensor State Symbols**
  It shows the aggregated status of all sensors you have configured for monitoring, divided into different sensor states. Depending on the sensors' status you will see colored boxes with numbers which symbolize the sensors. For example, you can see how many sensors are in **Up**, **Down**, or **Warning** state. Click on a box to view a list of all sensors in the respective status. For a detailed description, please see Sensor States 102 section.

Page Header Bar

In the page header under the global header area, you see the name of the current object and the page content underneath. When displaying a group, aggregated sensor states are shown in a sensor bar and there is an option to change the tree view.

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.



PRTG Page Header Bar with Heading, Tabs, Group Status Icons, and Tree View Selection

The page header and tabs area consists of the following parts:

- **Page Heading**
  The first line displays the kind of the current object and the name as page heading. In the screenshot above, it is the **Probe** named **Local probe** (which contains all objects on the local system). Next to the name, there are icons to pause or delete this object, or to add another object. By clicking on the arrow, you can open the context menu for this object with even more options. For more information, please see Context Menus 124 section.

- **Tabs**
  Using the tabs you can navigate to various sub-pages of an object, showing monitoring data or providing setting options. For more information, please see sections Review Sensor Data 104 and Change Device and Sensor Settings 111.

- **Sensor status bar**
  This element is only visible when viewing a probe or group. It is not available when viewing a device's or sensor's details. The sensor status bar shows the aggregated status of all sensors for the current object, divided into different sensor states. Depending on the sensors' status you will see colored squares with numbers which symbolize the sensors. For example, you can see how many sensors are in **Up**, **Down**, or **Warning** state. For a detailed description, please see Sensor States 102 section. You can hide sensors that are in a certain state by removing the check mark symbol in front of the respective sensor symbol. To show them again, re-add the check mark.

- **Tree view selection**
  This element is only visible when viewing a probe or group tree. It is not available when viewing a device's or sensor's details. You can select how much space is used to show devices and sensors. Switch between **S** (very condensed view), **M**, **L** or **XL** (extra large view).

Page Content

The page content of the general layout varies dependent on the selected object. It shows information about the current object and all other objects underneath in the tree hierarchy. The deeper down in the hierarchy you select an object, the more detailed is the displayed information.

By default, a **Probe Device** is created in the device tree on the local probe. It represents the probe system running with your PRTG installation. PRTG automatically monitors the system health of the core server and each probe in order to discover overloading situations that may distort monitoring results. To monitor the system status of the probe computer, PRTG automatically creates a few sensors. These include a Core/Probe Health Sensor 233, a WMI sensor that measures disk usage, and a bandwidth sensor for all installed network cards. It is recommended to keep these sensors, but you can optionally remove all except the **Core/Probe Health** sensor. In a cluster installation, PRTG also creates a **Cluster Probe Device** with a Cluster Probe Health Sensor 230 that monitors the cluster's system health.

For more details about page contents, please see the following sections:

- Review Monitoring Data 104
- Historic Data Reports 107
- Change Object Settings 111
- Compare Sensors 819

© 2011 Paessler AG

5.3 Sensor States

The sensors are the 'heart' of your PRTG installation. With sensors, you can monitor different aspects of your devices. Using a simple color code, they always show you what is going on with your devices.

The color of a sensor always shows it's current status. Following, you find a list of states a sensor can show.

Sensor	Color	Status Name	Meaning
	Red	**Down**	PRTG is not able to reach the device or the sensor has reached an error state. Another reason for this state can be a threshold trigger 801 set for this sensor.
	Red/Green	**Down (Partial)**	In a cluster, at least one node reports this sensor as **Down**, while at least one other node reports the same sensor as **Up**.
	Bright-Red	**Down (Acknowledged)**	The sensor is **Down** and the status was acknowledged by a PRTG user, applying the **Acknowledge Alarm** function. This can be helpful to mark that an alarm has already been attended to. For acknowledged alarms no more notifications 825 are sent. To set this sensor status, right-click on a sensor in a **Down** status and from the context menu 124, select **Acknowledge Alarm...**. Then enter a comment and click **OK**.
	Yellow	**Warning**	There was an error reading the sensor, but PRTG will try again. The sensor may soon change to a down status. Another reason for this state can be a threshold trigger 801 set for this sensor.
	Green	**Up**	The last check was okay and the sensor receives data.
	Blue	**Paused**	The sensor is currently paused (for a certain time, or unlimitedly).
	Orange	**Unusual**	The sensor reports unusual values for this weekday and time of day. The unusual detection is based on the historic average data and can be set in the system administration 871.
	Black	**Unknown**	The sensor has not been checked yet by PRTG or there is an error. If sensors show this state persistently, a PRTG restart may be necessary.

© 2011 Paessler AG

Sensor Warning and Down Behavior

The **Down** status symbolizes that something is wrong with a monitored device. There can be various reasons for a down status, e.g. an interruption in the physical connection to the device, an Internet connection outage, or simply a crashed server.

After a failed request, PRTG tries to reach the device again before setting a sensor to **Down** state (this is true for almost all types of sensors):

1. If a request to a device fails for the first time, the sensor is set to **Warning** state. PRTG repeats the request and tries to re-scan the device immediately.
2. If also the second request fails, the sensor is set to **Down** state until the device is reachable again. PRTG tries to reach the device with every scanning interval.

This procedure gives devices and services the chance to recover from a momentary overload and prevents false alarms. Still, you are informed promptly about any failures occurring.

5.4 Review Monitoring Data

Pages of probes, groups, device, and sensors have a tab-like interface. Using the tabs you can navigate through various sub-pages of an object in order to show your network's status, view monitoring results, or change settings.

Tabs Bar on Sensor Pages

Overview

The **Overview** tab shows an overview of the currently selected object and of its sensors. The pages share a common layout, but include different elements, depending on the kind of object you're looking at:

- For probes and groups, the **Overview** tab shows a tree with devices and sensors, as well as summary graphs for different time spans of the current probe or group.
- For devices, the **Overview** tab shows device details and summary graphs for different time spans, as well as a list of all sensors on this device.
- For sensors, the **Overview** tab shows sensor details, current status, and the last value of all sensor channels, as well as sensor graphs for different time spans.

Device Overview Tab for Probe Device with Overview, Sensor Table, GeoMap, and Mini Graphs

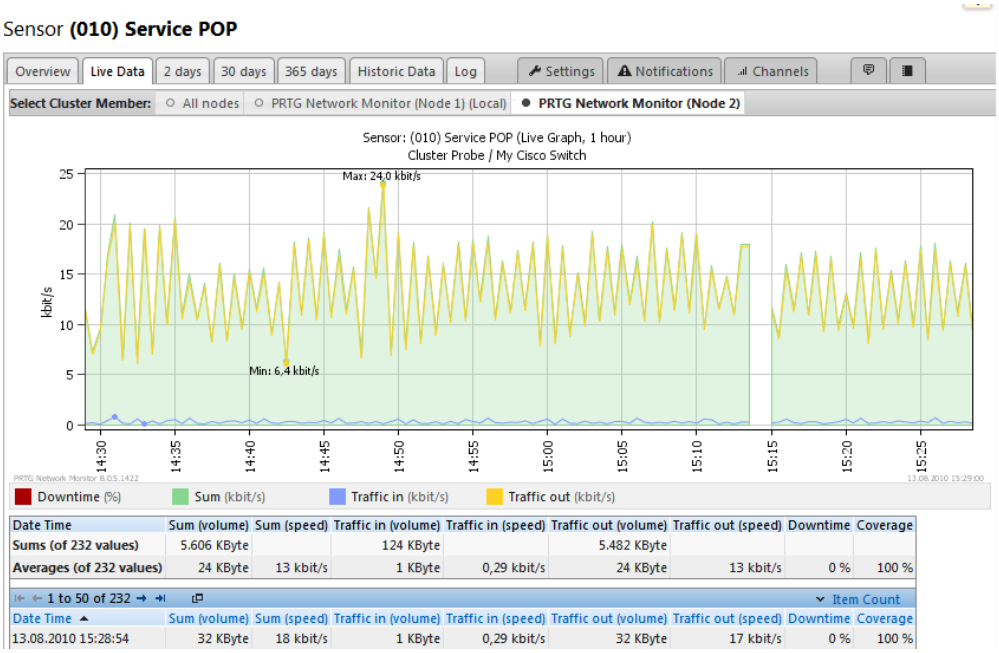
Live Data and Data By x Days

Select one of the tabs **Live Data** (available for sensors only), **2 days**, **30 days**, or **365 days** to display an object's monitoring data live (sensors only), or for different time spans and in more or less detail. *Note:* The days mentioned here are the default setting. You can change the detail of the different graphs any time in the PRTG System Administrator program. See section PRTG Server Administrator 960 (Memory Usage) for more details.

© 2011 Paessler AG

Group 2 Days Tab for Root Group with Group Graph and Sensor Mini Graphs

For probes, groups, and devices, each of the tabs shows a summary graph for the current object and mini graphs (2 days) for all sensors on this object, as well as a data table for the current object. There are never more than 50 mini graphs displayed for performance reasons.



Sensor Live Data Tab for a Traffic Sensor With Cluster Member Selection Bar

For sensors, the tabs show a graph and data table of the selected sensor. When viewing data of a sensor running on a cluster probe, you can additionally select if you want to show the data of all nodes, or of one specific node only. Please use the **Select Cluster Member** bar below the tabs. *Note:* Multi-node graphs are never displayed filled here, but with single lines only. However, historic data reports can have filled multi-node graphs.

Next to every graph, you will find two small icons. Using them, you can do the following:

- **Download the graph**: This will show a PNG file of the graph in a new browser window. You can then save or copy it for later use.
- **Zoom graph in new window**: This will open a larger version of the graph in a new browser window.

Toplists

The **Toplists** tab is available for xFlow and Packet Sniffer sensors 203 only. Please see section **Toplists** 807.

Historic Data

The **Historic Data** tab is available for sensors only. Please see section **Historic Data Reports** 107.

Sensors Lists

Viewing lists of sensors is a great way to keep an eye on your network's status, as you can select which kind of sensors you would like to see. There are many different sensor list views available, such as a list of favorite sensors and top 10 lists; lists filtered by current sensor status, value, availability, tag, or type; there is a sensor cross reference, and many more.

Sensor lists are available from the main menu. *Click* the **Sensors** entry to show a table list of all sensors. In the table list 119 appearing, you can re-sort the items by clicking on the column's header items. *Hover* to show other menu options. For detailed information about the available options, please see **Main Menu Structure** 135 (**Sensors**) section.

Alarms

The **Alarms** tab is not available for sensors, but for probes, groups, and devices only. Please see section **Alarms** 113.

Log

Please see section **Logs** 115.

Related Topics

- **Object Settings** 111
- **Compare Sensors** 819

© 2011 Paessler AG

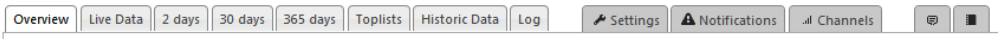
5.5 Historic Data Reports

For quick reporting on monitoring data, use historic data reports as an alternative to the exhaustive reports 827 function. You can view a report of the historic data for each single sensor, on demand. Additionally, you can also export this data and download it to you computer for further processing in external applications.

There are two possibilities to call the function for historic data reports: Either you click on the **Historic Data** tab on a sensor's detail page, or you choose **View Historic Data** from the **Sensors** entry in the main menu.

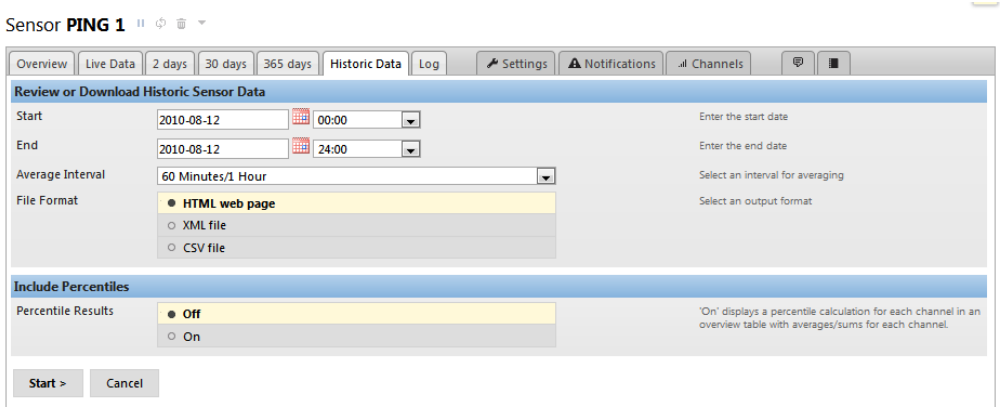
Historic Data (Sensor Tab)

Pages of probes, groups, device, and sensors have a tab-like interface. Using the tabs you can navigate through various sub-pages of an object in order to show your network's status, view monitoring results, or change settings.



Tabs Bar on Sensor Pages

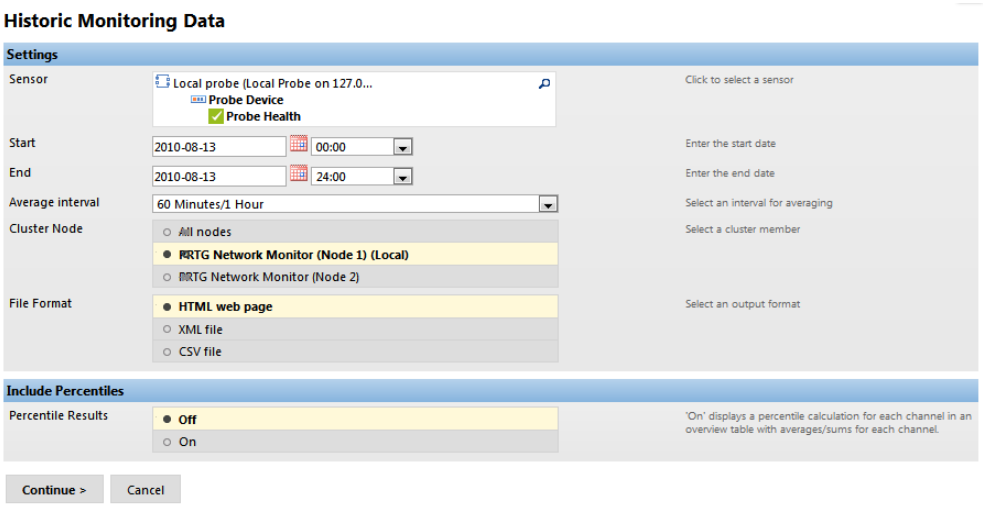
The **Historic Data** tab is available for sensors only (not for probes, groups, or devices). When calling the historic data reports via this tab, there is no sensor selection available, as you've already determined which sensor you would like to create a report for.



Historic Data Tab of a Ping Sensor

Historic Monitoring Data (Sensors Menu)

When calling the historic data reports via the **View Historic Data** entry from the **Sensors** entry in the main menu, an additional option is available, enabling you to choose the sensor you want to create a report for.



View Historic Data Function Called From Main Menu

Historic Data Reports Settings

Review or Download Historic Sensor Data	
Sensor	This field is only visible if you called this function via the main menu. Select the sensor you would like to create the report for: Click on the reading-glass symbol to open the object selector. For more information, please see section Object Selector 120.
Start	Enter the start date and time of the data you want to review.
End	Enter the end date and time of the data you want to review.
Average Interval	With this option, you can activate and set up averaging. Select an interval for which the average value should be calculated. You can choose between **No Interval** (no averaging will be performed), a few seconds, minutes, hours, or a whole day (**24 Hours**). A smaller interval will result in a more detailed report for this sensor. The best settings for you vary, depending on the scanning interval of the sensor, the selected date period and, of course, the intended use for the report. It might be useful to try different settings to see what the results look like. Please also see the section Automatic Averaging 109 below.
Cluster Node	This field is only visible if the sensor is running on a cluster probe.Select the cluster node's data that will be used for the report. Choose between: ▪ **All nodes**: Include the data of all cluster nodes in the report. ▪ ***[Several specific nodes]***: Use a specific node's data for the report. The nodes shown are specific to your setup.
File Format	Select the output format for the report. Choose between: ▪ **HTML web page**: Display the result directly as HTML web page. This is also a good option to check results before exporting to another file format.

© 2011 Paessler AG

Review or Download Historic Sensor Data	
	▪ **XML file**: Export the data as Extensible Markup Language (XML) file. Usually, you browser will show a download dialog. ▪ **CSV file**: Export the data as Comma Seperated Values (CSV) file, for example, for import in Microsoft Excel. Usually, you browser will show a download dialog.

Include Percentiles	
Percentile Results	Select if percentiles will be shown in the report. Choose between: ▪ **Off**: No percentiles will be calculated. ▪ **On**: Percentiles will be enabled in the report. In the overview table, additional values will be displayed with averages/sums for each sensor channel. Please define additional settings below. For more information about percentiles, please see section Calculating Percentiles 995.
Percentile	This field is only visible if percentile results are enabled above. Enter which percentile you would like to calculate. Please enter an integer value.
Percentile Average	This field is only visible if percentile results are enabled above. Enter the averaging interval in seconds that will be used for percentile calculation. Please enter an integer value.
Percentile Mode	This field is only visible if percentile results are enabled above. Choose between: ▪ **Discrete**: Chooses the next smaller discrete value. ▪ **Continuous**: Interpolates between discrete values.

Click on **Start** to start the generation of a historic data report.

Automatic Averaging

For performance reasons, PRTG automatically averages monitoring data when calculating data for large time spans. Data is then averaged regardless of the selected average interval.

Time Span in Report	Minimum Level of Detail (Average Interval)
Up to 40 days	Any
40 to 500 days	60 minutes/1 hour or larger

A report for a time span of more than 500 days is not possible. If you try to set a larger time span, it will be reduced to 365 days automatically.

Related Topics

- Review Monitoring Data 104

- Reports 827

© 2011 Paessler AG

5.6 Object Settings

Pages of probes, groups, device, and sensors have a tab-like interface. Using the tabs you can navigate through various sub-pages of an object in order to show your network's status, view monitoring results, or change settings.

Tabs Bar on Sensor Pages

General Settings

In the **Settings** tab you can define all settings of the current object. The available options vary, depending on the kind of object you're changing. Please see the following sections for information about the respective object types:

- Probe Settings 173
- Group Settings 181
- Device Settings 193
- Sensor Settings 202

The available setting options are different for *each* sensor, but always the same for probes, groups, and devices.

Notifications Settings

In the **Notifications** tab notification triggers can be set for every object. When using these settings for a probe, group, or device, they will be inherited to all sensors on these objects. Available notification trigger options are the same for all objects.

For more information, please see Sensor Notifications Settings 797 section.

Channels Settings

The **Channels** tab is available for sensors only. In the channel settings you can define how the data from the sensor's different channels are to be displayed in graphs and tables. Additionally, the channel data can affect the sensor's status. Use the limit settings to achieve this.

For more information, please see Sensor Channels Settings 792 section.

Comments

In the **Comments** tab you can enter free text for each object. This can be used for documentation purposes or to leave information for other users.

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the PRTG user which conducted the change, and a message. The history log is never purged.

Related Topics

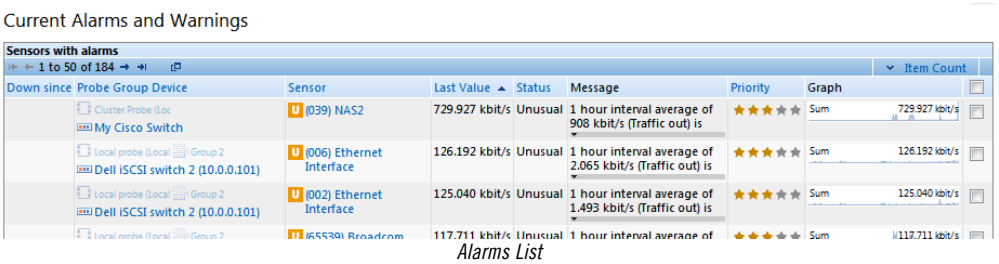
- General Layout 97
- Review Monitoring Data 104
- Toplists 807

© 2011 Paessler AG

5.7 Alarms

The Alarm list shows all sensors that are currently in a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. Sensors in other states (e.g. **Up**, **Paused**, or **Unknown**) do not appear here. This is useful to keep track of all irregularities in your network.

In the table list, you can re-sort the items by clicking on the column's header items.



Alarms List

There are two possibilities to call the alarms list: Either you click on the **Alarms** tab on the detail page of a probe, group, or device (not available for sensors), or you choose the **Alarms** entry in the main menu.

Alarms (Object Tab)

Pages of probes, groups, device, and sensors have a tab-like interface. Using the tabs you can navigate through various sub-pages of an object in order to show your network's status, view monitoring results, or change settings.

Tabs Bar on Object Pages

On an object's detail view, click on the **Alarms** tab to show a table list of all sensors *on this object* that currently show a **Down**, **Down (Partial)**, **Warning**, or **Unusual** status. You will see a subset of sensors in an alarm state for the current object only. This is a subset of the entries available via the **Alarms | All** option in main menu 137. The tab is not available on a sensor's detail page.

Alarms (Main Menu)

Click the **Alarms** entry from the main menu 137 to show a table list of *all* sensors in your configuration that currently show a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. *Hover* the **Alarms** entry and select another option to only show a subset of sensors in certain states. Choose between:

- **All**
  Shows a list of all sensors that currently show a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status.

- **Errors only**
  Shows a list of all sensors that currently show a **Down**, **Down (Partial)**, or **Down (Acknowledged)** status.

- **Warnings only**
  Shows a list of all sensors that currently show a **Warning** status.

- **Unusuals only**
  Shows a list of all sensors that currently show an **Unusual** status.

Acknowledge Alarm

An acknowledged alarm will not show up in the alarms list any more and will not trigger 797 any more notifications 825. In order to acknowledge an alarm, right-click on the respective sensor in a **Down** status that causes the alarm, and from the context menu 124, select **Acknowledge Alarm...**. Enter a comment that will be displayed next to the sensor's status and click **OK**.

© 2011 Paessler AG

5.8 Logs

The Logs list shows all past activities and events of your PRTG monitoring setup. This is useful to keep track of all important activities and, for example, to check whether messages were sent, etc. In a typical setup, a huge amount of data is produced here. As the activity of every single object is minuted, you can use this data to check exactly if your setup works as expected.

To support you when viewing the log files, there are several filters available. Please see Working with Table Lists 119 section for more information.

Log

1 to 50 of 521 (31.08.2010 - 01.09.2010) Date Range Item Count

Date Time	Parent	Type	Object	Status	Message	Cluster Node
31.08.2010 10:39:59	Poseidon 3268 (10.0.0.2...	Ping	PING 107	Up	0 msec	
31.08.2010 10:39:59	Poseidon 3268 (10.0.0.2...	Ping	PING 107	Warning	OK	
31.08.2010 10:37:14	None	Probe	Cluster Probe	Cluster	Access denied for node at 10.0.10.30:1234 (Incorrect software version)	PRTG Network Monitor (Node 1)
31.08.2010 10:35:12	CODZILLA	Ping	PING 12	Up	1 msec	
31.08.2010 10:34:54	CODZILLA	Ping	PING 12	Down	Request timed out (ICMP error # 11010)	

Logs List

There are two possibilities to call the logs list: Either you click on the **Log** tab on the detail page of a probe, group, device, or sensor, or you choose the **Logs** entry in the main menu.

Log (Object Tab)

Pages of probes, groups, device, and sensors have a tab-like interface. Using the tabs you can navigate through various sub-pages of an object in order to show your network's status, view monitoring results, or change settings.

Overview | 2 days | 30 days | 365 days | Alarms | Log | Settings | Notifications

Tabs Bar on Object Pages

On an object's detail view, click on the **Log** tab to show a table list with all log information *on this object*. This is a subset of the entries available via the **Logs | All** option in main menu 138.

Logs (Main Menu)

Click the **Logs** entry from the main menu 138 to show a table list of *all* log entries in your configuration. *Hover* the Logs entry and select another option to only show a subset of entries for certain objects for certain kind of entries. Choose between:

- **All**
  Show log information for all objects in your configuration, newest first.

- **By Group ›**
  Show log information for objects in a certain group only, newest first. *Hover* to show other menu items. Select **All,** or follow the menu path (it is specific to your setup) to select a group you would like to show log information for.

- **Status Changes ›**
  Show log information for certain status changes only. *Hover* to show other menu items. Follow the menu path to view log entries with a special value in the **Status** field only. Select between **Up & Down** (shows entries with either **Up** or **Down** in the **Status** field), **Down**, **Warning**, **Unusual**, **Up**, or **Paused/ Resumed** (shows entries with either **Paused** or **Resumed** in the **Status** field).

- **System Events ›**
  Show log information regarding certain system event types only. *Hover* to show other menu items. Select between the following event types: **Probe Related**, **Cluster Related**, **Auto-Discovery**, **Notifications**, or **Status Messages**.

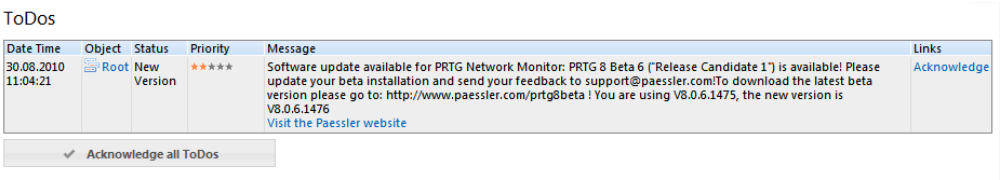
© 2011 Paessler AG

5.9 ToDos

The ToDos list shows items with important system information or action steps to take for the administrator.

New ToDos are created when:

- A new device or sensor has been created by the auto-discovery process and should be acknowledged by the user
- A new probe connects to the core and must be acknowledged
- A new cluster node connects to the cluster and must be acknowledged
- A new version of the software is available
- A new report is ready for review
- In a few other situations, such as when the system runs out of disk space, for licensing issues, etc.


ToDos
Date Time
Object
Status
Priority
Message
Links
30.08.2010 11:04:21
Root
New Version
Software update available for PRTG Network Monitor: PRTG 8 Beta 6 ("Release Candidate 1") is available! Please update your beta installation and send your feedback to support@paessler.com!To download the latest beta version please go to: http://www.paessler.com/prtg8beta ! You are using V8.0.6.1475, the new version is V8.0.6.1476
Visit the Paessler website
Acknowledge
Acknowledge all ToDos

ToDos List

Every ToDo should be viewed and acknowledged. By default, an email is sent to the administrator for every new ToDo that is created by the system. This can be changed in the system administration 871 (Email Options).

ToDos (Main Menu)

Click to show all ToDos with important system information or action steps to take for the administrator. In the table list appearing, you can filter the items by using the respective options 119. *Hover* to show other menu items. Choose between:

- **All**
  Shows all ToDos with important system information for the administrator.

- **Open ToDos**
  Shows all open ToDos, filtered by certain system event types. *Hover* to show other menu items. Select between the following event types: **Report Related**, **Auto-Discovery Related**, **Probe Related**, **Cluster Related**, **System Errors**, and **New Software Version**.

- **Acknowledged ToDos**
  Shows all already acknowledged ToDos, filtered by certain system event types. *Hover* to show other menu items. Select between the following event types: **Report Related**, **Auto-Discovery Related**, **Probe Related**, **Cluster Related**, **System Errors**, and **New Software Version**.

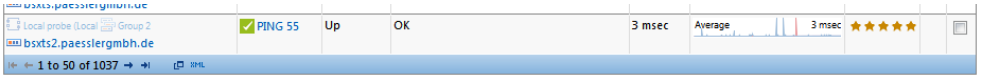
- **Acknowledge all ToDos**
  This option acknowledges all open ToDos. A warning popup is shown, asking you to confirm this action.

© 2011 Paessler AG

5.10 Working with Table Lists

Throughout the web interface often you will see table lists of items, e.g. of sensors, devices, maps, reports, etc. All these provide common functionality.

Start of List Example



End of List Example

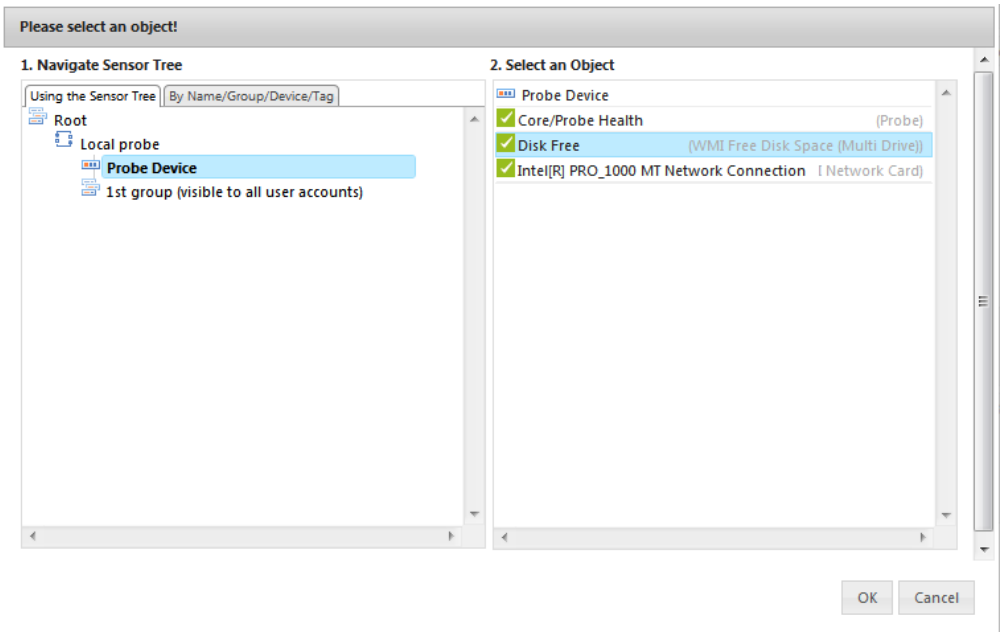
Feature	Display	What it does
Paging		The content of a table is displayed on several pages. Click on the arrow symbols at the beginning or the end of a list to view other pages, or to jump to the beginning or the end of the list.
New window		Click on the window symbol at the beginning or the end of a list to open the table in a new window.
Date Range	Date Range	When viewing log lists (not available in other lists), hover the **Date Range** option at the beginning of the list to select the time span you want to show log entries for. Choose between **Today**, **Yesterday**, and several other time spans. Choose **Unlimited** to disable this filter again.
Item Count	Item Count	Hover the **Item Count** option at the beginning of the list to select how many rows are shown on each page. Choose between **50**, **100**, and **500**.
Sorting	Priority	Click on the column headers to sort lists by the respective column. You can click on all blue words to sort, for example, by **Status**, **Last Value**, **Priority**, and more. The available options vary depending on the type of list.
Show XML	XML	Click on the **XML** option at the end of a list to download the current page in XML format. Your browser will usually show a download dialog.

Related Topics

- Multi-Edit Lists 813

5.11 Object Selector

For several functions, the object selector is shown. It enables you to browse all objects in your configuration and select an object in two steps.



Object Selector

Step 1: Navigate Sensor Tree

On the left hand side, you see a sensor tree specific to your setup. In the **Select using Sensor Tree** tab you can browse the sensor tree. Click on an object to view its details on the right hand side.

Click on the **By Name/Group/Device/Tag** tab to search for objects by sensor name, group name, device name, or by tag. Select the kind of object you want to search for and enter a few letters into the **Search String** box. This may be a substring only. The resulting objects will be displayed on the right side immediately. Hover an object on the right side to view its parent. Choose between the following search methods:

- **By Name**: Search for all object names. Shows matching probes, groups, devices, and sensors.
- **By Group**: Search for probe and group names. Shows matching groups and all devices and sensors for which a matching probe or group is the direct parent device.
- **By Device**: Search for device names. Shows matching devices and all sensors for which a matching device is the parent device.
- **By Tag**: Search for tags. Shows all matching objects. Tags can be inherited. See Tags 84 section for more details.

Step 2: Select an Object

If you have selected a device on the left hand side, you will see the sensors on this device here, on the right hand side. For sensors, also the sensor type is shown.

© 2011 Paessler AG

Select an object and click on the **OK** button.

5.12 Priority and Favorites

You can set priorities for all objects in your setup as well as mark devices or sensors as favorites. Both settings affect how your objects will be displayed. *Note:* Settings for priority and favorites are stored for the entire installation; they are not user specific.

Priority for All Objects

The priority setting will affect in which order your objects will be displayed when viewing lists. Objects with a higher priority are listed first, others underneath, depending on their own priority.

To change priority settings, right click on an object to open the context menu 124 and select **Priority**. You can now choose between 5 stars ***** (top priority) and one star * (lowest priority). By default, all objects are set to medium priority (3 stars ***).

Priority Context Menu

Favorites for Devices and Sensors

To call a list of all your favorite devices or sensors, select **Devices | Favorite Devices** or **Sensors | Favorite Sensors** from the main menu. These lists are sorted by priority as well.

You can mark any device or sensor as favorite to add it to the favorite list. Right click on it to open the context menu 124. Select **Priority/Favorite | Add to Favorites**. A small flag symbol will be added next to the object's name.

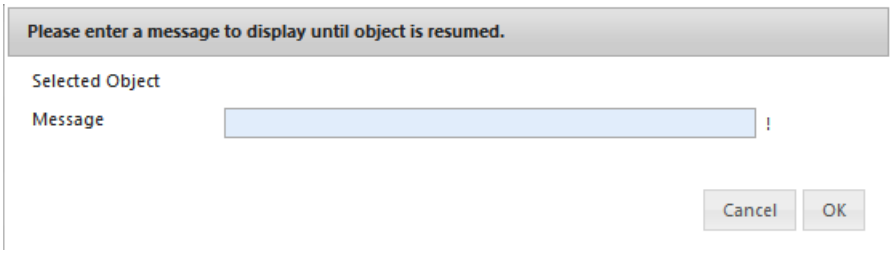
Priority/Favorites Context Menu

© 2011 Paessler AG

5.13 Pause

While a sensor is paused, it will not collect any monitoring data, will not change its status 102, and will not trigger any notifications 87. You can pause monitoring for every object by selecting **Pause** from the context menu 124 of a probe, a group, a device, or a sensor. All sensors on this object will then be paused. You can choose **Pause Indefinitely**, or select a time after which monitoring will be resumed automatically, such as **5** or **15 minutes**, **1** or **3 hours**, or **1 day**. When selecting the **Pause** symbol from an object's hover popup 132 it will be paused indefinitely until it is resumed.

When selecting a pause option, you are prompted to enter a message. This will be shown in the status message of the object as long as it is paused. Confirm with **OK** to pause the object; click **Cancel** to not pause it.



PRTG Pause Message Prompt

Inheritance and Resume

If you pause monitoring for an object in the device tree 97, all child objects underneath will be paused as well. For example, when pausing a group, all sensors on all devices in it will also be paused. Once an object is paused, you can resume monitoring any time by selecting **Resume** from the context menu 124. However, you cannot resume monitoring for single child objects that are paused by a parent object, but only for the object you originally set to pause. *Note:* Also after a restart of PRTG, a pause status will be kept.

5.14 Context Menus

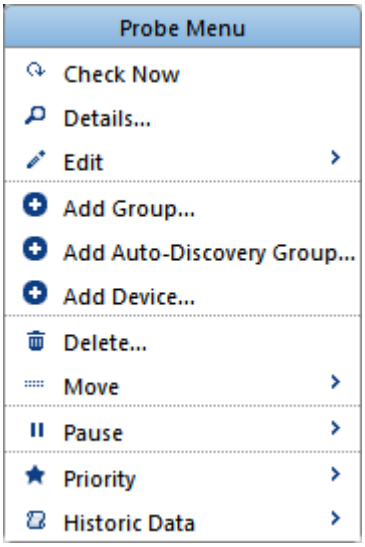
Right click on an object to view a context menu with many options for direct access to monitoring data and functions. You can also access many of the functionalities via the main menu 133 or the hover popup 132 window. However, using the context menus is the easier way in most cases.

Note: In order to view your browser's context menu, hold down the *Ctrl* key while right-clicking. You will then see your browser's instead of the PRTG menu.

The content of the PRTG context menu varies, depending on the type of object you have selected. Please see the following screen shots for an overview of the available options:

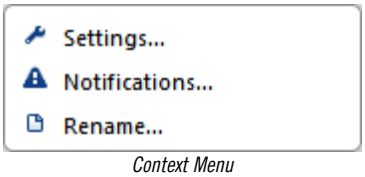
- Probe Context Menu 124
- Group Context Menu 125
- Device Context Menu 128
- Sensor Context Menu 130

Probe Context Menu



Context Menu

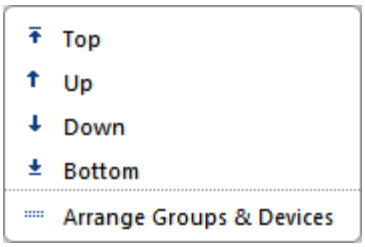
Edit ›



Context Menu

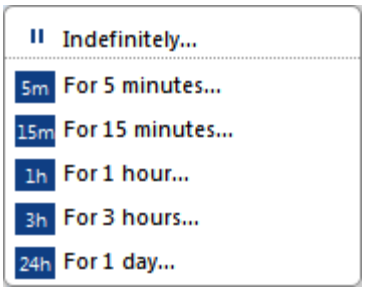
© 2011 Paessler AG

Move ›



Context Menu

Pause ›

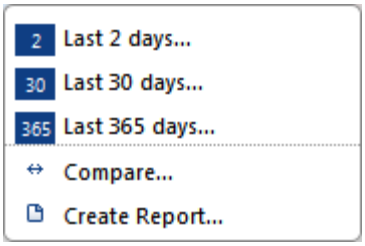


Context Menu

Priority ›

Context Menu

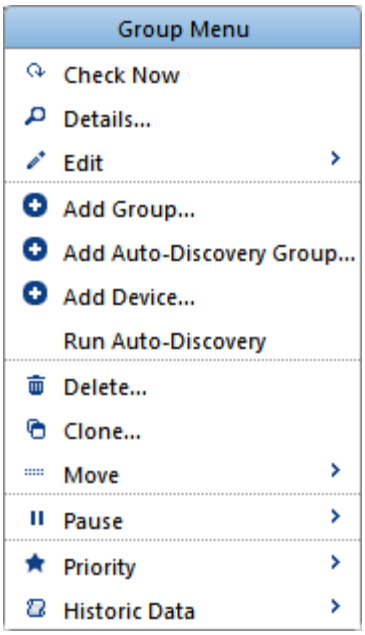
Historic Data ›



Context Menu

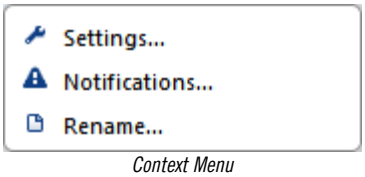
Group Context Menu

Note: The context menu of the **Root** group is special and differs from the other groups' menu.



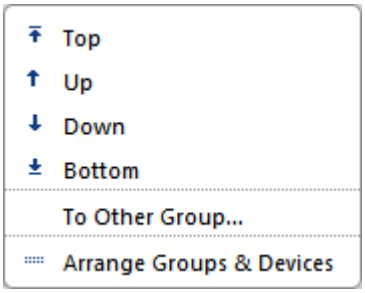
Context Menu

Edit ›



Context Menu

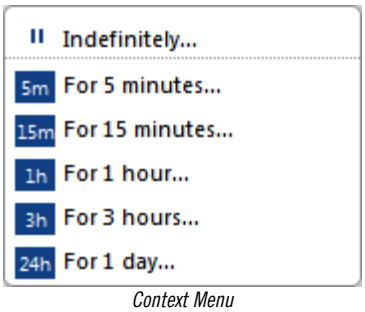
Move ›



Context Menu

© 2011 Paessler AG

Pause ›

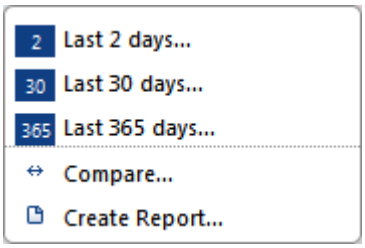


Context Menu

Priority ›

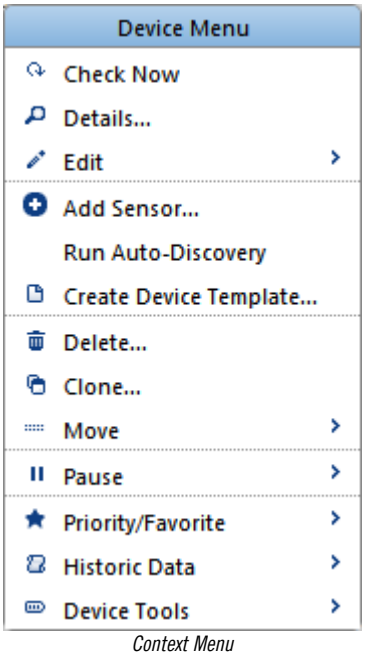
Context Menu

Historic Data ›



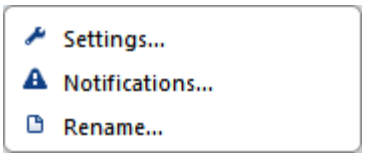
Context Menu

Device Context Menu



Context Menu

Edit ›



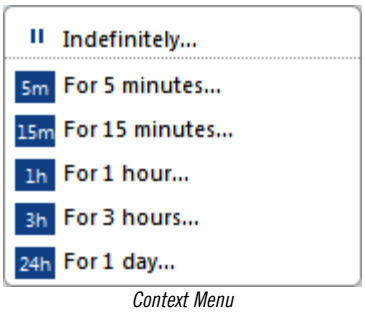
Context Menu

Move ›

Context Menu

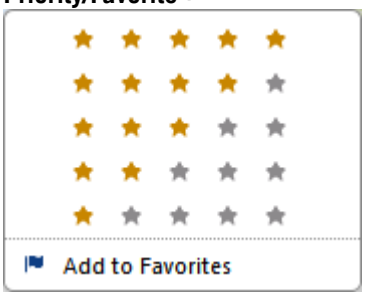
© 2011 Paessler AG

Pause ›



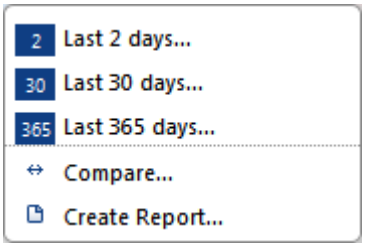
Context Menu

Priority/Favorite ›



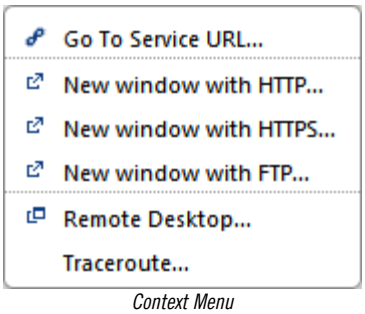
Context Menu

Historic Data ›



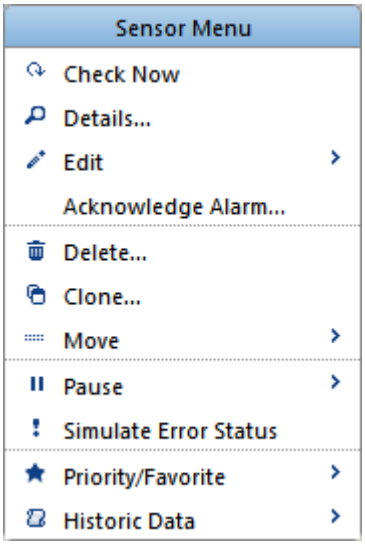
Context Menu

Device Tools ›



Context Menu

Sensor Context Menu



Context Menu

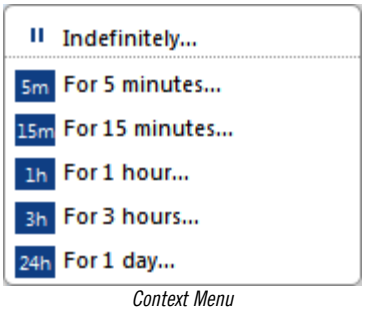
Edit ›

Context Menu

Move ›

Context Menu

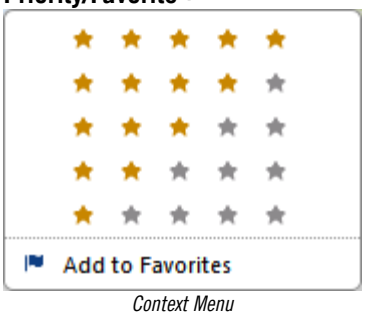
Pause ›



Context Menu

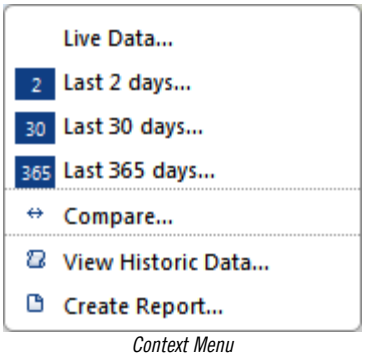
© 2011 Paessler AG

Priority/Favorite ›



Context Menu

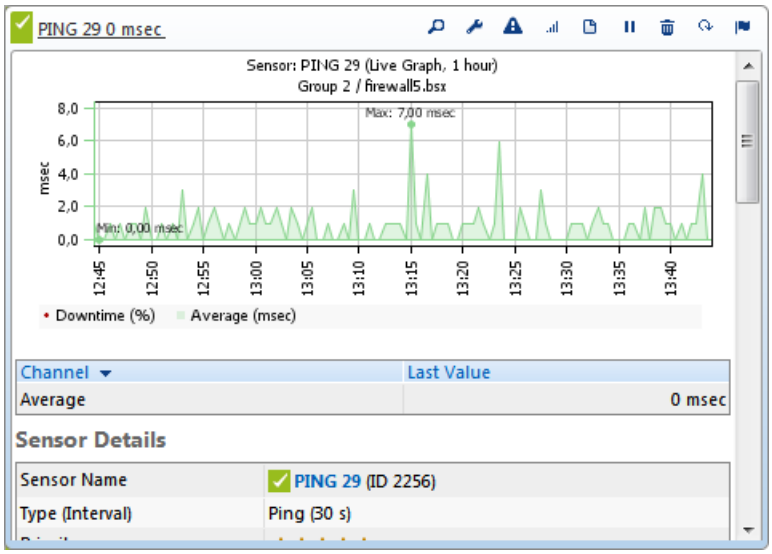
Historic Data ›



Context Menu

5.15 Hover Popup

Whenever you rest the mouse pointer for a second over an object in the device tree 97, a hover popup window with details about this object will be shown. It contains information from the object's overview tab 104, as well as several graphs. The exact information provided depends on the kind of object you are hovering.



Hover Menu Example: Ping Sensor

Note: The hover popup does only appear when your browser is the currently focused window on your desktop. It disappears with every (automatic) page refresh. Hover popups are only available for definite objects, not for cumulated sensor icons showing names like *12 Sensors* or similar.

Menu Icons

At the top of the hover popup window, several icons are shown which enable you to view or edit the current object. These are the most important options from this object's context menu 124 which is shown when right-clicking it.

© 2011 Paessler AG

5.16 Main Menu Structure

Using the main menu, you can access all functions of PRTG. Following, the most important menu items are described. Often, you can either *click* on an item directly, or *hover* it to show more items.

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

The following menu items are available:

- Home 133
- Devices 134
- Sensors 135
- Alarms 137
- Maps 137
- Reports 138
- Logs 138
- ToDos 139
- Setup 139
- Refresh (Arrows Symbol) 140
- Help Center (? Symbol) 140
- Logout (Off Symbol) 140
- Search Box 140

Home

Click to open the user's homepage. The default setting is PRTG's welcome page. The homepage can be changed in the user's account settings 859. *Hover* to show other menu items.

- **Dashboard 1 – Dashboard 4**
  The dashboards provide different preset overviews with the status of your sensors. Choose the one that fits your needs. **Dashboard 4** is optimized for mobile access. It is opened in a new window and includes no navigation in order to provide as much space as possible. *Note:* Dashboards are not customizable. You can create your own overview pages using the Maps 842 feature.

- **Sitemap**
  The sitemap contains a flat text view of all menu items. You can easily search for key words using the search function in your browser (usually shortcut *CTRL-F*).

- **Welcome to PRTG**
  Shows the welcome screen which leads you to the major sections of the web interface.

- **Make This My Homepage**
  Change the page that is loaded when you click on the **Home** button in the main menu. Select this menu item on any page and its URL will be set as the current user's homepage immediately. This setting is user sensitive. The default homepage is */welcome.htm*. You can change this setting any time by clicking on this menu item again, or by changing the **Homepage URL** in the **My Account** 859 settings.

- **Go to HTML Interface**
  This switches to the HTML GUI 927 optimized for low bandwidth and mobile devices. Less scripting is used for more compatibility. However, this is a read-only interface.

Devices

Click to show a group view of all your devices, starting with the **Root** group which contains all other groups of your setup. *Hover* to show other menu items.

- **Group View ›**
  Shows a tree view of all probes and groups in your setup. *Click* to show a group view of all your devices, starting with the **Root** group which contains all other groups of your setup. *Hover* to show other menu items. Follow the menu path (it is specific to your setup) to view the devices in a specific probe or group only.

- **Device List ›**
  Shows a list view of all devices in your setup. *Click* to show a table list of all devices in your setup. *Hover* to show other menu items. Choose **Favorite Devices** to show a list of all devices marked as Favorite 122. *Note:* To mark any device as a favorite device, select **Priority/Favorite | Toggle Favorite** from its context menu. Follow the menu path (it is specific to your setup) to view a table list of the devices in a specific probe or group only. In the table list 119 appearing, you can re-sort the items by clicking on the column's header items.

- **Dependencies ›**
  Shows an overview of the dependencies configured for the objects in your setup. *Hover* the menu item to show other menu items. Follow the menu path (it is specific to your setup) to view dependencies of the objects in a specific probe or group only.

- **Add Group**
  Start an assistant which guides you through the process of adding a new group to your setup. For more information, please see section Create Objects Manually 156. *Tip:* You can create new groups much faster by choosing **Add Group...** from a probe's or group's context menu!

- **Add Auto-Discovery Group**
  Start an assistant which guides you through the process of adding a new auto-discovery group to your setup. PRTG will create a new group and run an auto-discovery in your network in order to add devices and sensors for these devices automatically. For more information, please see section Using the Auto-Discovery 145 *Tip:* You can create new groups much faster by choosing **Add Auto-Discovery Group...** from a probe's or group's context menu!

- **Add Device**
  Start an assistant which guides you through the process of adding a new device to an existing group. During the process, you can choose if PRTG should run an auto-discover for the new device in order to add sensors automatically. For more information, please see section Create Objects Manually 156. *Tip:* You can create new devices much faster by choosing **Add Device...** from a group's context menu!

- **Arrange Probes & Groups**
  Opens a table list of probes and groups in which you can rearrange the display order of these items using drag and drop. For more information, please see Arrange Objects 811 section.

© 2011 Paessler AG

- **Arrange Groups & Devices ›**
  Opens a table list of groups and devices in which you can rearrange the display order of these items using drag and drop. For more information, please see Arrange Objects 811 section.

Sensors

Click to show a table list of all sensors. In the table list appearing, you can re-sort the items by clicking on the column's header items. *Hover* to show other menu items.

- **All**
  Shows a table list of all sensors. In the table list appearing, you can re-sort the items by clicking on the column's header items.

- **Add Sensor**
  Start an assistant which guides you through the process of adding a new sensor to an existing device. For more information, please see section Add a Sensor 165. During the process, you can also choose to create a new device. This will bring you to the "Add Device" assistant you can call from the "Devices" menu directly.

- **Favorite Sensors**
  Shows a table list of all sensors marked as Favorite 122. *Note:* To mark any sensor as a favorite sensor, select **Priority/Favorite | Toggle Favorite** from its context menu.

- **Top 10 Lists ›**
  This is an option to show a filtered sensor list. *Click* to show an overview with various Top 10 lists for all sensors. *Hover* to show other menu items. Follow the menu path (it is specific to your setup) to view Top 10 table lists for a specific probe or group only.

- **By Current Value ›**
  This is an option to show a filtered sensor list. *Hover* to show other menu items. Follow the menu path to view table lists of several sensor types sorted by **Fastest**, **Slowest**, **Most Used**, and **Least Used**.

- **By Current Status ›**
  This is an option to show a filtered sensor list. *Hover* to show other menu items. Follow the menu path to view table lists of all sensors in a certain state. Select between status **Up**, **Warning**, **Down**, **Unusual**, **Paused**, and **Unknown**. For more information about sensor states, please see Sensor States 102 section.

- **By Uptime/Downtime ›**
  This is an option to show a filtered sensor list. *Hover* to show other menu items. Follow the menu path to view table lists of all sensors sorted by their up- or downtime. Select between **Best Uptime (%)**, **Highest Uptime (Time)**, **Worst Downtime (%)**, and **Highest Downtime (Time)**.

- **By Group ›**
  This is an option to show a filtered sensor list. *Hover* to show other menu items. Follow the menu path (it is specific to your setup) to view a sensor table list of a specific probe or group only.

- **By Type ›**
  This is an option to show a filtered sensor list. *Hover* to show other menu items. Follow the menu path (it is specific to your setup) to view a sensor table list containing only sensors of one specific sensor type.

- **By Tag ›**
  This is an option to show a filtered sensor list. *Hover* to show other menu items. Follow the alphabetical menu path (it is specific to your setup) to see available tags. Select a tag view a table list containing only sensors marked with this tag.

© 2011 Paessler AG

- **Cross Reference ›**
  The cross reference shows information about all sensors including the set interval, access rights, notification trigger settings, schedule, and dependency. *Click* to show a sensor cross reference for all sensors. *Hover* to show other menu items. Follow the menu path (it is specific to your setup) to view cross reference information for sensors in a specific probe or group only.

- **Compare Sensors**
  Calls a function to compare graphs of two monitoring objects. For more information, please see Compare Sensors 819 section.

- **View Historic Data**
  Calls a function for quick generation of sensor data reports. For more information, please see Historic Data Reports 107 section.

Alarms

Click to show a table list of all sensors that currently show a **Down**, **Down (Partial)**, **Warning**, or **Unusual** status. In the table list 119 appearing, you can re-sort the items by clicking on the column's header items. *Hover* to show other menu items.

- **All**
  Shows a list of all sensors that currently show a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status.

- **Errors only**
  Shows a list of all sensors that currently show a **Down**, **Down (Partial)**, or **Down (Acknowledged)** status.

- **Warnings only**
  Shows a list of all sensors that currently show a **Warning** status.

- **Unusuals only**
  Shows a list of all sensors that currently show an **Unusual** status.

Maps

Click to call the Maps feature where you can view or add custom views of your network's status and monitoring data. For more information, please see Maps 842 section. *Hover* to show other menu items.

- **All**
  Calls the Maps feature where you can view or add custom views of your network's status and monitoring data.

- **Add Map**
  Lets you directly add 845 a new map.

- **Select Map ›**
  Show existing maps. *Hover* to show other menu items. Follow the menu path (it is specific to your setup) to select a map.

Reports

Click to call the Reports feature where you can view or add reports of your monitoring data. For more information, please see **Reports** 827 section. *Hover* to show other menu items.

- **All**
  Calls the Reports feature where you can view or add reports of your monitoring data.

- **Add Report**
  Lets you directly add a new report.

- **Select Report ›**
  Show existing reports. *Hover* to show other menu items. Follow the menu path (it is specific to your setup) to select a report.

Logs

Click to show log information for all objects in your configuration, newest first. In the table list 119 appearing, you can filter the items by using the respective options 119. *Hover* to show other menu items. For more information, please see **Logs** 115 section.

- **All**
  Show log information for all objects in your configuration, newest first.

- **By Group ›**
  Show log information for objects in a certain group only, newest first. *Hover* to show other menu items. Select **All,** or follow the menu path (it is specific to your setup) to select a group you would like to show log information for.

- **Status Changes ›**
  Show log information for certain status changes only. *Hover* to show other menu items. Follow the menu path to view log entries with a special value in the **Status** field only. Select between **Up & Down** (shows entries with either **Up** or **Down** in the **Status** field), **Down**, **Warning**, **Unusual**, **Up**, or **Paused/ Resumed** (shows entries with either **Paused** or **Resumed** in the **Status** field).

- **System Events ›**
  Show log information regarding certain system event types only. *Hover* to show other menu items. Select between the following event types: **Probe Related**, **Cluster Related**, **Auto-Discovery**, **Notifications**, or **Status Messages**.

© 2011 Paessler AG

ToDos

Click to show all ToDos with important system information or action steps to take for the administrator. Every ToDo should be viewed and acknowledged. In the table list 119 appearing, you can filter the items by using the respective options 119. *Hover* to show other menu items. For more information, please see **ToDos** 117 section.

- **All**
  Shows all ToDos with important system information for the administrator.

- **Open ToDos**
  Shows all open ToDos, filtered by certain system event types. *Hover* to show other menu items. Select between the following event types: **Report Related**, **Auto-Discovery Related**, **Probe Related**, **Cluster Related**, **System Errors**, and **New Software Version**.

- **Acknowledged ToDos**
  Shows all already acknowledged ToDos, filtered by certain system event types. *Hover* to show other menu items. Select between the following event types: **Report Related**, **Auto-Discovery Related**, **Probe Related**, **Cluster Related**, **System Errors**, and **New Software Version**.

- **Acknowledge all ToDos**
  This option acknowledges all open ToDos. A warning popup is shown, asking you to confirm this action.

Setup

Click to show the setup page. *Hover* to show other menu items. For more information, please see **Setup** 857 section.

- **Overview**
  Shows the setup page.

- **Account Settings ›**
  Hover to show menu items of the account settings. Select between: **My Account**, **Notifications**, and **Schedules**.

- **System Administration ›**
  Hover to show menu items of the system administration settings. Select between: **System & Website**, **Notification Delivery**, **Probes**, **Cluster**, **User Accounts**, and **User Groups**.

- **PRTG Status ›**
  Hover to show menu items of the PRTG status. Select between: **System Status**, **Cluster Status**, and **Activation Status**.

- **Downloads**
  Shows additional downloads for PRTG. Select between: **PRTG Windows GUI**, **iPRTG iPhone App**, **Remote Probe Installer**, and **PRTG Add-Ons**.

- **PRTG API**
  Show the API 979 documentation for your installation.

- **Enter License Key**
  Shows help on how to enter a license key 55.

Refresh (Arrows Symbol)

Click this symbol to refresh all elements on the current page to display current data. Unlike the reload function of your browser, this merely refreshes the single page elements, not the whole page. During the refresh process, this symbol flashes.

Help Center (? Symbol)

Shows the help center which supports you if you have any questions regarding your PRTG setup.

Logout (Off Symbol)

Logs out the current user and shows the login screen 94.

Search Box

Use the search box to find objects and reports, and other items by name or tag, or to search for help.

Context Menu

Additionally, there is a context menu 124 available for every object. Right-click on an object to open it.

© 2011 Paessler AG

Part VI

Ajax Web Interface—Device and Sensor Setup

6 Ajax Web Interface—Device and Sensor Setup

The Ajax-based web interface is your access to PRTG. It is used to configure devices and sensors, and to set up notifications, as well as review monitoring results and create reports. This web interface is highly interactive and uses Asynchronous Java Script and XML (AJAX) to deliver a powerful and easy-to-use user experience. While the user is logged in 93, the data on the screen is permanently refreshed (via Ajax calls) so it always shows the current monitoring results (refresh interval and method can be set 884 by the user).

The following sections introduce device and sensor setup in the Ajax Graphical User Interface (GUI).

Ajax Web Interface—Device and Sensor Setup—Topics

- Auto-Discovery 145
- Create Objects Manually 156
- Root Group Settings 166
- Probe Settings 173
- Group Settings 181
- Device Settings 193
- Sensor Settings 202—List of Available Sensor Types 203
- Sensor Channels Settings 792
- Sensor Notifications Settings 797

Other Ajax Web Interface Sections

- Ajax Web Interface—Basic Procedures 92
- Ajax Web Interface—Advanced Procedures 806

Related Topics

- Windows GUI 894
- Other User Interfaces 926

© 2011 Paessler AG

6.1 Auto-Discovery

PRTG's auto-discovery function is a great way to automatically create a sophisticated and concise set of sensors for your complete network. It is mainly suitable for LAN discovery since it involves a lot of SNMP and WMI. For video instructions, please see the More 155 section below.

For a quick start auto-discovery, please see THREE—Auto-Discover Your Network 32 section.

How Auto-Discovery Works

PRTG's auto-discovery process has three stages:

- **Step 1**
  Scanning a network segment for devices using Ping (for groups only).

- **Step 2**
  Assessing the device type for all devices discovered in Step 1 (using SNMP, WMI and other protocols).

- **Step 3a**
  Creating sensor sets that match the discovered device types of step 2. This is done based on built-in device templates with recommended sensors for many device types.

  Step 3b (optional)
  Creating sensor sets using user created device templates (see Create Device Template 815 section).

The auto-discovery can be used on a group level for a range of IP addresses, or for individual devices you might have created manually. It can be run just once, on demand via the context menu, or scheduled every hour, day or week. Running the auto-discovery every day or week will automatically create new sensors when new devices are connected to the network. As soon as new devices or sensors are discovered, new ToDos 117 are created (which are usually mailed to the system administrator).

Please be aware of the following restrictions of the auto-discovery:

- PRTG can not discover devices that can not be pinged, since Step 1 uses pings. If, for example, a firewall blocks echo requests, a device behind it cannot be discovered.
- You should supply authentication settings for **Windows Systems**, **Linux (SSH/WBEM) Systems**, **VMware/XEN Servers**, and **SNMP Devices** in order to fully exploit the power of this feature. We recommend defining these in the Root group settings 166.
- If a device has more than one IP address, it may show up more than once in the discovery results, even though PRTG tries to identify these situations.
- Using frequent auto-discoveries of large network segments can lead to performance issues. We therefore recommend to only schedule regular auto-discoveries where necessary. For detailed information see the More 155 section below.

Run Auto-Discovery Now

You can run an auto-discovery any time for a group or a device. To do so, right-click on the respective object and from the context menu, select **Run Auto-Discovery**. PRTG will immediately start searching for new objects it can add. If used for a group, PRTG will add devices and sensors, if found. If used for a device, it will add new sensors, if found.

Note: The auto-discovery will also re-add devices or sensors you have manually deleted. If you do not want this, please create objects manually 156 only.

Creating an Auto-Discovery Group

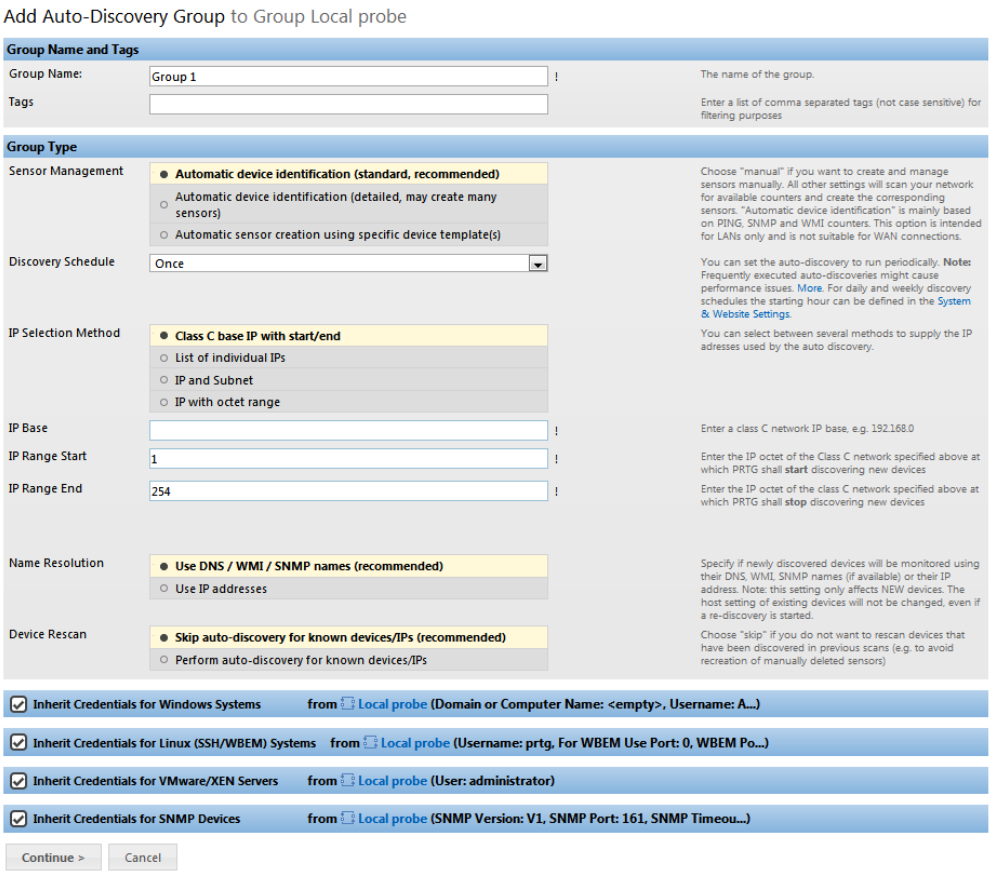
There are several ways to start auto-discovery:

- On the welcome screen 97, click on the **Perform Network Auto-Discovery** option
- or select **Devices | Add Auto-Discovery Group** from the main menu.

To start an automatic detection of devices and sensors in your network. An assistant will appear, leading you through two steps. For faster setup, you can select **Add Auto-Discovery Group...** in the context menu 124 of a probe or group to which you want to add the new group. This will skip step 1 and lead you directly to step 2.

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

© 2011 Paessler AG


Add Auto-Discovery Group to Group Local probe
Group Name and Tags
Group Name:
Group 1
The name of the group.
Tags
Enter a list of comma separated tags (not case sensitive) for filtering purposes
Group Type
Sensor Management
Automatic device identification (standard, recommended)
Automatic device identification (detailed, may create many sensors)
Automatic sensor creation using specific device template(s)
Choose "manual" if you want to create and manage sensors manually. All other settings will scan your network for available counters and create the corresponding sensors. "Automatic device identification" is mainly based on PING, SNMP and WMI counters. This option is intended for LANs only and is not suitable for WAN connections.
Discovery Schedule
Once
You can set the auto-discovery to run periodically. Note: Frequently executed auto-discoveries might cause performance issues. More. For daily and weekly discovery schedules the starting hour can be defined in the System & Website Settings.
IP Selection Method
Class C base IP with start/end
List of individual IPs
IP and Subnet
IP with octet range
You can select between several methods to supply the IP adresses used by the auto discovery.
IP Base
Enter a class C network IP base, e.g. 192.168.0
IP Range Start
1
Enter the IP octet of the Class C network specified above at which PRTG shall start discovering new devices
IP Range End
254
Enter the IP octet of the class C network specified above at which PRTG shall stop discovering new devices
Name Resolution
Use DNS / WMI / SNMP names (recommended)
Use IP addresses
Specify if newly discovered devices will be monitored using their DNS, WMI, SNMP names (if available) or their IP address. Note: this setting only affects NEW devices. The host setting of existing devices will not be changed, even if a re-discovery is started.
Device Rescan
Skip auto-discovery for known devices/IPs (recommended)
Perform auto-discovery for known devices/IPs
Choose "skip" if you do not want to rescan devices that have been discovered in previous scans (e.g. to avoid recreation of manually deleted sensors)
Inherit Credentials for Windows Systems from Local probe (Domain or Computer Name: <empty>, Username: A...)
Inherit Credentials for Linux (SSH/WBEM) Systems from Local probe (Username: prtg, For WBEM Use Port: 0, WBEM Po...)
Inherit Credentials for VMware/XEN Servers from Local probe (User: administrator)
Inherit Credentials for SNMP Devices from Local probe (SNMP Version: V1, SNMP Port: 161, SNMP Timeou...)
Continue >
Cancel

Add Auto-Discovery Group Assistant Step 2

- **Step 1**
  Please choose a probe or group you want to add the new group to. Click on **Continue**.

- **Step 2**
  Add auto-discovery settings as described below.

Add Auto-Discovery Group Settings

Group Name and Tags	
Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Group Type	
Sensor Management	Select the method for automatic network discovery. Choose between:

Group Type	
	▪ **Automatic device identification (standard, recommended)**: Detect mainly based on Ping, SNMP, and WMI. This option should work fine for most installations. ▪ **Automatic device identification (detailed, may create many sensors)**: Detect in a more detailed way and create more sensors. This option uses all standard device templates for auto-discovery. It is suitable for small network segments and whenever you want to monitor the maximum number of sensors available. ▪ **Automatic sensor creation using specific device template(s)**: Manually define the device templates used for auto-discovery. From the list below, select one or more templates.
Device Template(s)	This option is only available if using specific device templates is enabled above. Choose one or more device templates from the list by adding a check mark in front of the respective template name. Choose from: ▪ **Cisco Device (Generic)** ▪ **DNS Server** ▪ **FTP Server** ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **HTTP Web Server** ▪ **Hyper V Host Server** ▪ **Linux/UNIX Device (SNMP or SSH enabled)** ▪ **LocalhostRDP** ▪ **Mail Server (Generic)** ▪ **Mail Server (MS Exchange 2003)** ▪ **Mail Server (MS Exchange 2007)** ▪ **Misc. Details** ▪ **Printer (HP)** ▪ **Server (Compaq/HP agents)** ▪ **Switch (Cisco Catalyst)** ▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)** ▪ **UNIX/Linux Device** ▪ **UPS (APC)** ▪ **VMware ESX Server** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)** ▪ **XEN Server**
Discovery Schedule	Define when the auto-discovery will be run. Choose between: • **Once**: Perform auto-discovery only once. New devices and sensors will be added once. You can run auto-discovery manually any time using an object's context menu 124. • **Hourly**: Perform auto-discovery for new devices and sensors every 60 minutes. *Note:* Please use this option with caution! Frequently executed auto-discoveries might cause performance issues, especially when large network segments are scanned every hour.

© 2011 Paessler AG

Device Template(s)	This option is only available if using specific device templates is enabled above. Choose one or more device templates from the list by adding a check mark in front of the respective template name. Choose from: ▪ **Cisco Device (Generic)** ▪ **DNS Server** ▪ **FTP Server** ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **HTTP Web Server** ▪ **Hyper V Host Server** ▪ **Linux/UNIX Device (SNMP or SSH enabled)** ▪ **LocalhostRDP** ▪ **Mail Server (Generic)** ▪ **Mail Server (MS Exchange 2003)** ▪ **Mail Server (MS Exchange 2007)** ▪ **Misc. Details** ▪ **Printer (HP)** ▪ **Server (Compaq/HP agents)** ▪ **Switch (Cisco Catalyst)** ▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)** ▪ **UNIX/Linux Device** ▪ **UPS (APC)** ▪ **VMware ESX Server** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)** ▪ **XEN Server**
	• **Daily**: Perform auto-discovery for new devices and sensors every 24 hours. The first auto-discovery will run immediately, all other discoveries will start on the time defined in the **Auto-Discovery Settings** section of the System Administration—System and Website 871 settings. • **Weekly**: Perform auto-discovery for new devices and sensors every 7 days. The first auto-discovery will run immediately, all other discoveries will start on the time defined in the **Auto-Discovery Settings** section of the System Administration—System and Website 871 settings.
IP Selection Method	Define how you want to define the IP range for auto-discovery. Choose between: ▪ **Class C base IP with start/end**: Define a class C address range. ▪ **List of individual IPs**: Enter individual IP addresses. ▪ **IP and subnet**: Enter an IP address and subnet mask. ▪ **IP with octet range**: Enter an IP address range for every IP octet individually. With this, you can define very customizable IP ranges. *Note:* Only subnets with up to 65,536 IP addresses can be discovered! If you define a range with a higher number of addresses, discovery will stop before it is completed.
IP Base	This field is only visible if Class C network detection is selected above. Enter a class C network as IP base for the auto-discovery. Enter the first three octets of an IPv4 IP address, for example, **192.168.0**

Device Template(s)	This option is only available if using specific device templates is enabled above. Choose one or more device templates from the list by adding a check mark in front of the respective template name. Choose from: ▪ **Cisco Device (Generic)** ▪ **DNS Server** ▪ **FTP Server** ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **HTTP Web Server** ▪ **Hyper V Host Server** ▪ **Linux/UNIX Device (SNMP or SSH enabled)** ▪ **LocalhostRDP** ▪ **Mail Server (Generic)** ▪ **Mail Server (MS Exchange 2003)** ▪ **Mail Server (MS Exchange 2007)** ▪ **Misc. Details** ▪ **Printer (HP)** ▪ **Server (Compaq/HP agents)** ▪ **Switch (Cisco Catalyst)** ▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)** ▪ **UNIX/Linux Device** ▪ **UPS (APC)** ▪ **VMware ESX Server** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)** ▪ **XEN Server**
IP Range Start	This field is only visible if Class C network detection is selected above. Enter the IP octet of the class C network specified above from which PRTG will start the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter **1** to discover from **192.168.0.1**.
IP Range End	This field is only visible if Class C network detection is selected above. Enter the IP octet of the class C network specified above at which PRTG will stop the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter **254** to discover up to **192.168.0.254**.
IP List	This field is only visible if the IP list option is selected above. Enter a list of IP addresses which the auto-discovery will scan. Enter each address in a separate line.
IP and Subnet	This field is only visible if the IP and subnet option is selected above. Enter an expression in the format **address/subnet**, e.g. *192.168.3.0/255.255.255.0*. You can also use the short form like *192.168.3.0/24* in this example. PRTG will scan the complete host range (without network and broadcast address) defined by the IP address and the subnet mask.

© 2011 Paessler AG

Device Template(s)	This option is only available if using specific device templates is enabled above. Choose one or more device templates from the list by adding a check mark in front of the respective template name. Choose from: ▪ **Cisco Device (Generic)** ▪ **DNS Server** ▪ **FTP Server** ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **HTTP Web Server** ▪ **Hyper V Host Server** ▪ **Linux/UNIX Device (SNMP or SSH enabled)** ▪ **LocalhostRDP** ▪ **Mail Server (Generic)** ▪ **Mail Server (MS Exchange 2003)** ▪ **Mail Server (MS Exchange 2007)** ▪ **Misc. Details** ▪ **Printer (HP)** ▪ **Server (Compaq/HP agents)** ▪ **Switch (Cisco Catalyst)** ▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)** ▪ **UNIX/Linux Device** ▪ **UPS (APC)** ▪ **VMware ESX Server** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)** ▪ **XEN Server**
IP with Octet Range	This field is only visible if the octet range option is selected above. Enter an expression in the format **a1.a2.a3.a4**, where *a1*, *a2*, *a3*, and *a4* are each a number between 0-255, or a range with two numbers and a hyphen like *1-127*. All permutations of all ranges are calculated, e.g. *10.0.1-10.1-100* results in 1,000 addresses that PRTG will scan during auto-discovery.
Name Resolution	Define how newly discovered devices will be monitored. This only affects *new* devices. The setting for existing devices will be kept. Choose between: • **Use DNS / WMI / SNMP names (recommended)**: Monitor newly discovered devices via their DNS, WMI, or SNMP names (if available). • **Use IP addresses**: Monitor newly discovered devices via their IP address. We recommend using the default value.
Device Rescan	Define if you want to rescan known devices. Choose between: • **Skip auto-discovery for known devices/IPs (recommended)**: Do not re-scan known devices or IP addresses, but only scan for new devices/IPs when auto-discovering. This can avoid re-creation of manually deleted sensors. PRTG will also avoid adding devices that are already included elsewhere in your configuration, e.g. in other groups.

Device Template(s)	This option is only available if using specific device templates is enabled above. Choose one or more device templates from the list by adding a check mark in front of the respective template name. Choose from: ▪ **Cisco Device (Generic)** ▪ **DNS Server** ▪ **FTP Server** ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **HTTP Web Server** ▪ **Hyper V Host Server** ▪ **Linux/UNIX Device (SNMP or SSH enabled)** ▪ **LocalhostRDP** ▪ **Mail Server (Generic)** ▪ **Mail Server (MS Exchange 2003)** ▪ **Mail Server (MS Exchange 2007)** ▪ **Misc. Details** ▪ **Printer (HP)** ▪ **Server (Compaq/HP agents)** ▪ **Switch (Cisco Catalyst)** ▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)** ▪ **UNIX/Linux Device** ▪ **UPS (APC)** ▪ **VMware ESX Server** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)** ▪ **XEN Server**
	• **Perform auto-discovery for known devices/IPs**: Re-scan known devices and IP addresses with every auto-discovery. This will re-create manually deleted sensors on existing devices. We recommend using the default value.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

If you have not set credentials yet, set them now before starting the auto-discovery in order to fully exploit the power of this feature!

Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other sensors. If using a Windows local user account, please enter the computer name here. If using a Windows domain user account, please enter the domain name here.

© 2011 Paessler AG

Credentials for Windows Systems	
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.
Credentials for Linux (SSH/WBEM) Systems	
Username	Enter a login name for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Password	Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **HTTP**: Use an unencrypted connection for WBEM. • **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. • **Set manually**
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
Credentials for VMware/XEN Servers	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Choose between: • **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XEN servers. • **HTTP**: Use an unencrypted connection to VMware and XEN servers.
Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between: • **v1**: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. • **v2c**: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. • **v3**: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption.

Credentials for SNMP Devices	
	Note for SNMP v3: Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version **v1** or **v2c** are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: • **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication. • **SHA**: Use Secure Hash Algorithm (SHA) for authentication. Your device must be set to the same value.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. Your device must be set to the same value.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. Your device must be set to the same value.
Data Encryption Key (DES)	This setting is only visible if SNMP version v3 is enabled above. Enter a Data Encryption Standard (DES) key here. If you provide a key in this field, SNMP data packets will be enrypted using the DES encryption algorithm, providing increased security. Your device must be set to the same value. *Note:* If the key entered in this field does not match the key configured in the target SNMP device you will not get an error message! Please enter a string or leave the field empty.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Auto-Discovery in Progress

While auto-discovery is running you may experience a lower system performance as usual, because PRTG works in the background in order to discover your network. Depending on the IP ranges defined (up to 65,536 addresses) , the discovery may run up to several days before complete. You can review the status of the discovery process as follows:

© 2011 Paessler AG

- In the sensor tree, behind the group or device name, you will see a percentage value showing the progress of auto-discovery.
- During auto-discovery, the web interface will display a box in the lower right corner, showing the number of active auto-discovery tasks.
- In order to stop a running auto-discovery, right-click the group or device, and select **Pause | For 5 minutes...** from the context menu 124. Monitoring will be paused for 5 minutes, and auto-discovery tasks will be shut down.

Related Topics

- **Create Device Template** 815

More

Video Tutorial: There is a video available on the Paessler video tutorials page.
- http://www.paessler.com/support/video_tutorials

Knowledge Base: Why can automatic auto-discoveries evoke performance issues?
- http://www.paessler.com/knowledgebase/en/topic/14423

Knowledge Base: Why are sensors missing in my auto-created device template?
- http://www.paessler.com/knowledgebase/en/topic/5853

6.2 Create Objects Manually

We recommend using the auto-discovery 145 function to create a basic monitoring setup for your network. Afterwards, you can manually create devices that could not be discovered, or arrange 811 detected devices in groups.

The procedure depends on the kind of object you want to add. Choose between:

- **Add a Remote Probe** 156
- **Add a Group** 157
- **Add a Device** 160
- **Add a Sensor** 165

Add a Remote Probe

Please see **Multiple Probes and Remote Probes** 986 section for more information.

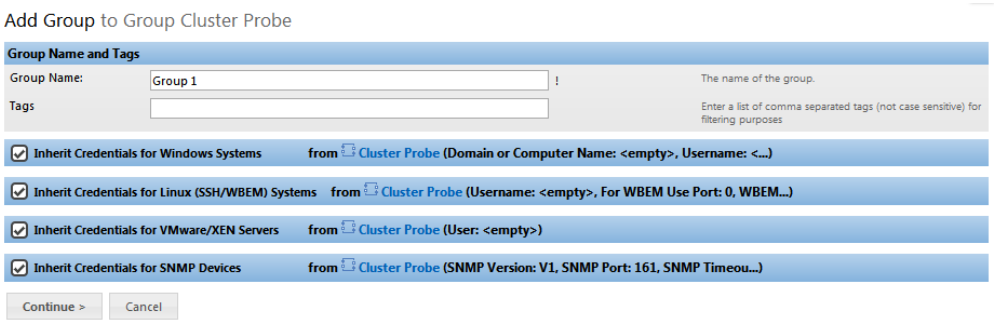
© 2011 Paessler AG

6.2.1 Add a Group

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

To manually add a group, select **Devices | Add Group** from the main menu. An assistant will appear, leading you through two steps. For faster setup, you can select **Add Group...** in the context menu 124 of a probe or group to which you want to add the new group. This will skip step 1 and lead you directly to step 2.

- **Step 1**
  Please choose a probe or group you want to add the new group to. Click on **Continue**.


Add Group to Group Cluster Probe
Group Name and Tags
Group Name:
Group 1
The name of the group.
Tags
Enter a list of comma separated tags (not case sensitive) for filtering purposes
Inherit Credentials for Windows Systems from Cluster Probe (Domain or Computer Name: <empty>, Username: <...)
Inherit Credentials for Linux (SSH/WBEM) Systems from Cluster Probe (Username: <empty>, For WBEM Use Port: 0, WBEM...)
Inherit Credentials for VMware/XEN Servers from Cluster Probe (User: <empty>)
Inherit Credentials for SNMP Devices from Cluster Probe (SNMP Version: V1, SNMP Port: 161, SNMP Timeou...)
Continue >
Cancel

Add Group Assistant Step 2

- **Step 2**
  Add group settings as described below.

Add Group Settings

Group Name and Tags	
Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other sensors. If using a Windows local user account, please enter the computer name here. If using a Windows domain user account, please enter the domain name here.
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.

Credentials for Windows Systems	
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.
Credentials for Linux (SSH/WBEM) Systems	
Username	Enter a login name for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Password	Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **HTTP**: Use an unencrypted connection for WBEM. • **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. • **Set manually**
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
Credentials for VMware/XEN Servers	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Choose between: • **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XEN servers. • **HTTP**: Use an unencrypted connection to VMware and XEN servers.
Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between: • **v1**: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. • **v2c**: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. • **v3**: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption.

© 2011 Paessler AG

Credentials for SNMP Devices	
	Note for SNMP v3: Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version **v1** or **v2c** are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: • **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication. • **SHA**: Use Secure Hash Algorithm (SHA) for authentication. Your device must be set to the same value.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. Your device must be set to the same value.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. Your device must be set to the same value.
Data Encryption Key (DES)	This setting is only visible if SNMP version v3 is enabled above. Enter a Data Encryption Standard (DES) key here. If you provide a key in this field, SNMP data packets will be enrypted using the DES encryption algorithm, providing increased security. Your device must be set to the same value. *Note:* If the key entered in this field does not match the key configured in the target SNMP device you will not get an error message! Please enter a string or leave the field empty.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

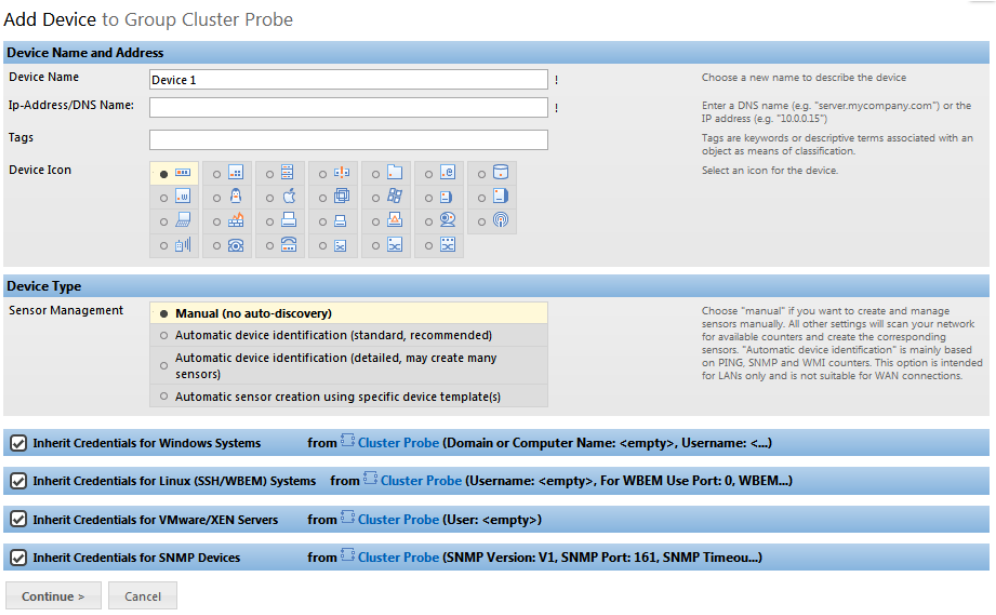
Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

6.2.2 Add a Device

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

To manually add a device, select **Devices | Add Device** from the main menu. An assistant will appear, leading you through two steps. For faster setup, you can select **Add Device...** in the context menu 124 of a group to which you want to add the new device. This will skip step 1 and lead you directly to step 2.

- **Step 1**
  Please choose a group you want to add the new device to. Click on **Continue**.


Add Device to Group Cluster Probe
Device Name and Address
Device Name
Device 1
Choose a new name to describe the device
Ip-Address/DNS Name:
Enter a DNS name (e.g. "server.mycompany.com") or the IP address (e.g. "10.0.0.15")
Tags
Tags are keywords or descriptive terms associated with an object as means of classification.
Device Icon
Select an icon for the device.
Device Type
Sensor Management
Manual (no auto-discovery)
Automatic device identification (standard, recommended)
Automatic device identification (detailed, may create many sensors)
Automatic sensor creation using specific device template(s)
Choose "manual" if you want to create and manage sensors manually. All other settings will scan your network for available counters and create the corresponding sensors. "Automatic device identification" is mainly based on PING, SNMP and WMI counters. This option is intended for LANs only and is not suitable for WAN connections.
Inherit Credentials for Windows Systems from Cluster Probe (Domain or Computer Name: <empty>, Username: <...)
Inherit Credentials for Linux (SSH/WBEM) Systems from Cluster Probe (Username: <empty>, For WBEM Use Port: 0, WBEM...)
Inherit Credentials for VMware/XEN Servers from Cluster Probe (User: <empty>)
Inherit Credentials for SNMP Devices from Cluster Probe (SNMP Version: V1, SNMP Port: 161, SNMP Timeou...)
Continue >
Cancel

Add Device Assistant Step 2

- **Step 2**
  Add device settings as described below.

Add Device Settings

Device Name and Address	
Device Name	Enter a meaningful name to identify the device. The name will be shown by default in the sensor tree and in all alarms.
IP Address/DNS Name	Enter the IP address or DNS name for the device. Most sensors created on this device will inherit this setting and they will try to connect to this address for monitoring. (However, some sensor types still have their own setting for IP address/DNS name.)

© 2011 Paessler AG

Device Name and Address	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Device Icon	Choose a device icon from the list. It will be shown in the device tree.
Device Type	
Sensor Management	Select which type of auto-discovery you would like to perform for this device. Choose between: ▪ **Manual (no auto-discovery)**: Do not auto-discover any sensors, but only add sensors manually. ▪ **Automatic device identification (standard, recommended)**: Use a small set of auto-discovery templates. This will scan your LAN and usually create a view standard sensors on your device. ▪ **Automatic device identification (detailed, may create many sensors**: Use an extended set of auto-discovery templates. This will scan your LAN and usually create many sensors on your device. ▪ **Automatic sensor creation using specific device templates**: Use specific auto-discovery templates only. Please select templates below. This will scan your LAN and add sensors defined in the template.
Discovery Schedule	This option is only visible if one of the auto-discovery options is selected above. Define when the auto-discovery will be run. Choose between: ▪ **Once**: Perform auto-discovery only once. For existing devices, this will initiate a one-time sensor update for the current device. ▪ **Hourly**: Perform auto-discovery for new sensors every hour. ▪ **Daily**: Perform auto-discovery for new sensors every day. ▪ **Weekly**: Perform auto-discovery for new sensors every week.
Device Template(s)	This option is only visible if using specific device templates (last option) is enabled above. Please choose one or more templates by adding a check mark in front of the respective template name. These will be used for auto-discovery on the current device. Choose from: ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **Generic Device (SNMP-enabled)** ▪ **VMware ESX Server** ▪ **Hyper V Host Server** ▪ **Printer (HP)** ▪ **DNS Server** ▪ **FTP Server** ▪ **Server (Compaq/HP agents)** ▪ **HTTP Web Server** ▪ **Mail Server (MS Exchange 2007)** ▪ **Mail Server (MS Exchange 2003)** ▪ **Mail Server (Generic)** ▪ **Switch (Cisco Catalyst)** ▪ **Switch (Cisco Generic)** ▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)**

Device Type	
	▪ **UNIX/Linux Device** ▪ **UPS (APC)** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)**
Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other sensors. If using a Windows local user account, please enter the computer name here. If using a Windows domain user account, please enter the domain name here.
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.
Credentials for Linux (SSH/WBEM) Systems	
Username	Enter a login name for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Password	Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **HTTP**: Use an unencrypted connection for WBEM. • **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. • **Set manually**
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
Credentials for VMware/XEN Servers	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Choose between: • **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XEN servers.

© 2011 Paessler AG

Credentials for VMware/XEN Servers	
	• **HTTP**: Use an unencrypted connection to VMware and XEN servers.
Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between: • **v1**: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. • **v2c**: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. • **v3**: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption. *Note for SNMP v3:* Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version **v1** or **v2c** are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: • **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication. • **SHA**: Use Secure Hash Algorithm (SHA) for authentication. Your device must be set to the same value.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. Your device must be set to the same value.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. Your device must be set to the same value.
Data Encryption Key (DES)	This setting is only visible if SNMP version v3 is enabled above. Enter a Data Encryption Standard (DES) key here. If you provide a key in this field, SNMP data packets will be enrypted using the DES encryption algorithm, providing increased security. Your device must be set to the same value. *Note:* If the key entered in this field does not match the key configured in the target SNMP device you will not get an error message! Please enter a string or leave the field empty.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.

Credentials for SNMP Devices	
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

© 2011 Paessler AG

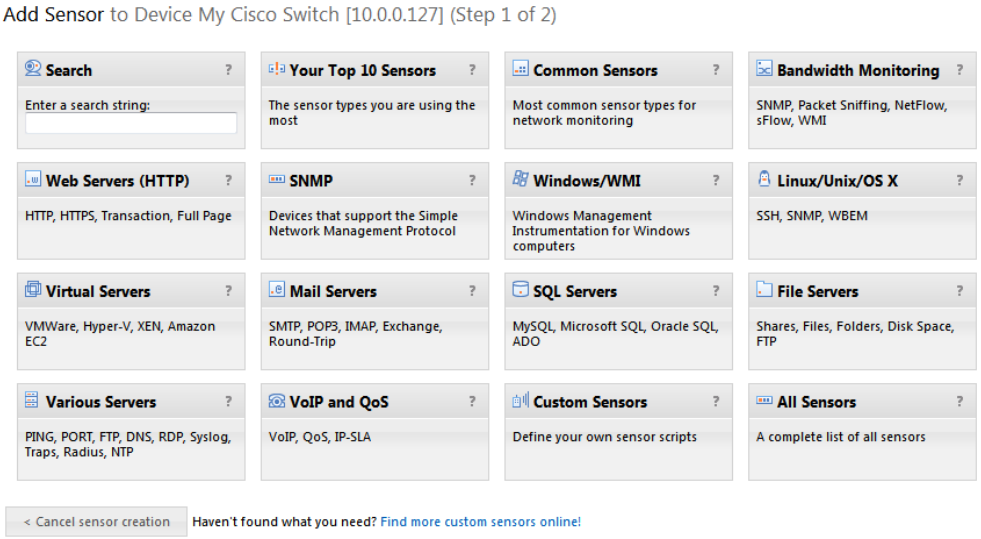
6.2.3 Add a Sensor

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

There are different ways to manually add a sensor to an existing device.

- On the welcome screen 97, click on the **Add Sensors Manually** option
- or select **Sensors | Add Sensor** from the main menu.

An assistant will appear, leading you through two steps. For faster setup, you can select **Add Sensor...** in the context menu 124 of a device to which you want to add the new sensor. This will skip step 1 and lead you directly to step 2.


Add Sensor to Device My Cisco Switch [10.0.0.127] (Step 1 of 2)
Search
Enter a search string:
Your Top 10 Sensors
The sensor types you are using the most
Common Sensors
Most common sensor types for network monitoring
Bandwidth Monitoring
SNMP, Packet Sniffing, NetFlow, sFlow, WMI
Web Servers (HTTP)
HTTP, HTTPS, Transaction, Full Page
SNMP
Devices that support the Simple Network Management Protocol
Windows/WMI
Windows Management Instrumentation for Windows computers
Linux/Unix/OS X
SSH, SNMP, WBEM
Virtual Servers
VMWare, Hyper-V, XEN, Amazon EC2
Mail Servers
SMTP, POP3, IMAP, Exchange, Round-Trip
SQL Servers
MySQL, Microsoft SQL, Oracle SQL, ADO
File Servers
Shares, Files, Folders, Disk Space, FTP
Various Servers
PING, PORT, FTP, DNS, RDP, Syslog, Traps, Radius, NTP
VoIP and QoS
VoIP, QoS, IP-SLA
Custom Sensors
Define your own sensor scripts
All Sensors
A complete list of all sensors
< Cancel sensor creation
Haven't found what you need? Find more custom sensors online!

Add Sensor Assistant

- **Step 1**
  Please select **Add sensor to an existing device** and choose a device you want to add the new sensor to. Click on **Continue**.

- **Step 2**
  The Add sensor assistant is shown (see screenshot above). Select a sensor you want to add and enter the needed settings. For more information, please see the manual section of the respective sensor. See **List of Available Sensor Types** 203 section to find detailed information about every sensor.

6.3 Root Group Settings

On the **Root** group's overview page, click on the **Settings** tab to change settings.

The Root Group is Special

The **Root** group is the highest instance in the object hierarchy of your PRTG setup and parent to all other objects. Therefore all objects inherit settings from the **Root** group. If you define important settings on this high level, work will be easier later on. So, before you create your own sensors, it is a good idea to review the **Root** group's settings to ensure they suit your network. There are already reasonable presets made with installation.

Note: If necessary, you can override every setting for every single child object later. To do so, simply disable the respective **Inherit** option of an object.

Root Group Settings

The following settings are available in the **Settings** tab. As you may not need all of these, just regard those settings you really need, ignoring the others. All settings you define here can easily be inherited to all other objects in your setup.

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Basic Group Settings	
Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Status	Define if monitoring for this group is started or paused. Choose between: • **Started**: Monitor this group. • **Paused**: Pause monitoring for this group. All sensors on all devices in this group will be paused until this setting is changed again.

Location	
Location (for geo maps)	When using geo maps using Google's API 823 please enter a location in the first line. Objects will then be displayed on a geographical map with a flag, showing the current status using a color code similar to the sensor status icons 102 (green - yellow - red). You can enter a full postal address, city and country only, or latitude and longitude here. A minus sign (-) will hide an object from geo maps.

© 2011 Paessler AG

Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other sensors. If using a Windows local user account, please enter the computer name here. If using a Windows domain user account, please enter the domain name here.
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.
Credentials for Linux (SSH/WBEM) Systems	
Username	Enter a login name for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Password	Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **HTTP**: Use an unencrypted connection for WBEM. • **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. • **Set manually**
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
Credentials for VMware/XEN Servers	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Choose between: • **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XEN servers. • **HTTP**: Use an unencrypted connection to VMware and XEN servers.
Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between:

Credentials for SNMP Devices	
	• **v1**: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. • **v2c**: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. • **v3**: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption. *Note for SNMP v3:* Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version **v1** or **v2c** are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: • **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication. • **SHA**: Use Secure Hash Algorithm (SHA) for authentication. Your device must be set to the same value.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. Your device must be set to the same value.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. Your device must be set to the same value.
Data Encryption Key (DES)	This setting is only visible if SNMP version v3 is enabled above. Enter a Data Encryption Standard (DES) key here. If you provide a key in this field, SNMP data packets will be enrypted using the DES encryption algorithm, providing increased security. Your device must be set to the same value. *Note:* If the key entered in this field does not match the key configured in the target SNMP device you will not get an error message! Please enter a string or leave the field empty.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
WMI Compatibility Options	
When experiencing problems while monitoring via Windows Management Instrumentation (WMI) sensors, you can set some compatibility options for trouble shooting.	

© 2011 Paessler AG

WMI Compatibility Options	
Timeout method	Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between: • **Use 1.5x scanning interval (recommended)**: Use a default of one and a half times the scanning interval set for the sensor (see below in this settings). • **Set manually**: Enter a timeout value manually. We recommend using the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.
Timeout value (sec.)	This field is only visible if manually timeout method is selected above. Specify the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value.
RPC server port	Specify the port which WMI uses for DCOM communication. We recommend using the default value. Only if you change this port on your system(s), please change it here.
SNMP Compatibility Options	
When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for trouble shooting.	
SNMP Delay (ms)	Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend using the default value. If you experience SNMP connection failures, please increase it.
Failed Requests	Define if an SNMP sensor will try again after a request fails. • **Retry (recommended)**: Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures. • **Do not retry**: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be put to error state earlier.
Overflow Values	Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks. • **Ignore overflow values (recommended)**: Ignore overflow values and do not include them in the monitoring data. • **Handle overflow values as valid results**: Regard all overflow values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
Zero Values	Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks. • **Ignore zero values for delta sensors (recommended)**: Ignore zero values and do not include them in the monitoring data. • **Handle zero values as valid results for delta sensors**: Regard all zero values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
32-bit/64-bit Counters	Define which kind of traffic counters PRTG will search for on a device.

SNMP Compatibility Options	
	• **Use 64-bit counters if available (recommended)**: The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices. • **Use 32-bit counters only**: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices. We recommend using the default value. If you experience problems, change this option.
Request Mode	Define which kind of request method PRTG uses for SNMP sensors. • **Use multi get (recommended)**: Bundle multiple SNMP requests into one request. • **Use single get**: Use one request for each SNMP value. This can increase compatibility with older devices. We recommend using the default value. If you experience problems, change this option.
Port Name Template	Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device/OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, **([port]) [ifalias]** is set as port name template, which will create a name such as *(001) Ethernet1*, for example. You can use any field names available at a certain OID of your device, among which are: • **[port]** • **[ifalias]** • **[ifname]** • **[ifindex]** • **[ifdescr]** Combine them as you like to obtain suitable sensor names. See the **More** section below for more information about SNMP sensor names.
HTTP Proxy Settings	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Please enter a string or leave the field empty.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current object will be dependent on.
Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.
Unusual Detection	
Unusual Detection	Define if unusual detection is enabled for sensors. You can set the behavior of unusual detection in the system settings. • **Enabled**: Enable unusual detection. Sensors will turn to orange color if unusual activity is detected. • **Disabled**: Disable unusual detection. To not use the orange sensor color.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to you needs. In an object's detail page, click on the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?
▪ http://www.paessler.com/knowledgebase/en/topic/313

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?
▪ http://www.paessler.com/knowledgebase/en/topic/7313

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?
▪ http://www.paessler.com/knowledgebase/en/topic/7363

© 2011 Paessler AG

6.4 Probe Settings

On a probe's overview page, click on the **Settings** tab to change settings.

Add Remote Probe

You can add additional remote probes to your setup to extend you monitoring to networks that are not directly reachable by your PRTG core installation or cluster.

See Add Remote Probe 986 section for more details.

Probe Settings

The following settings are available in the **Settings** tab of every probe. As you may not need all of these for every probe, just regard those settings you really need, ignoring the others.

We recommend defining as many settings as possible in the Root 166 group, so you can inherit them to all other objects further down in the tree hierarchy.

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Basic Probe Settings	
Probe Name	Enter a meaningful name to identify the probe. The name will be shown by default in the devices tree and in all alarms.
Status	Choose if monitoring for this probe is started or paused. • **Started**: Monitor this probe. • **Paused**: Pause monitoring for this probe. All sensors on all devices on this probe will be paused until this setting is changed again.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like.
Priority	Select a priority for the probe. This setting determines where the probe will be placed in list views. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Location	
Location (for geo maps)	When using geo maps using Google's API 823 please enter a location in the first line. Objects will then be displayed on a geographical map with a flag, showing the current status using a color code similar to the sensor status icons 102 (green - yellow - red). You can enter a full postal address, city and country only, or latitude and longitude here. A minus sign (-) will hide an object from geo maps.
Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other sensors. If using a Windows local user account, please enter the computer name here. If using a Windows domain user account, please enter the domain name here.
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.
Credentials for Linux (SSH/WBEM) Systems	
Username	Enter a login name for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Password	Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **HTTP**: Use an unencrypted connection for WBEM. • **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. • **Set manually**
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
Credentials for VMware/XEN Servers	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Choose between:

© 2011 Paessler AG

Credentials for VMware/XEN Servers	
	• **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XEN servers. • **HTTP**: Use an unencrypted connection to VMware and XEN servers.
Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between: • **v1**: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. • **v2c**: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. • **v3**: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption. *Note for SNMP v3:* Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version **v1** or **v2c** are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: • **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication. • **SHA**: Use Secure Hash Algorithm (SHA) for authentication. Your device must be set to the same value.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. Your device must be set to the same value.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. Your device must be set to the same value.
Data Encryption Key (DES)	This setting is only visible if SNMP version v3 is enabled above. Enter a Data Encryption Standard (DES) key here. If you provide a key in this field, SNMP data packets will be enrypted using the DES encryption algorithm, providing increased security. Your device must be set to the same value. *Note:* If the key entered in this field does not match the key configured in the target SNMP device you will not get an error message! Please enter a string or leave the field empty.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.

Credentials for SNMP Devices	
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
WMI Compatibility Options	
When experiencing problems while monitoring via Windows Management Instrumentation (WMI) sensors, you can set some compatibility options for trouble shooting.	
Timeout method	Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between: • **Use 1.5x scanning interval (recommended)**: Use a default of one and a half times the scanning interval set for the sensor (see below in this settings). • **Set manually**: Enter a timeout value manually. We recommend using the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.
Timeout value (sec.)	This field is only visible if manually timeout method is selected above. Specify the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value.
RPC server port	Specify the port which WMI uses for DCOM communication. We recommend using the default value. Only if you change this port on your system(s), please change it here.
SNMP Compatibility Options	
When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for trouble shooting.	
SNMP Delay (ms)	Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend using the default value. If you experience SNMP connection failures, please increase it.
Failed Requests	Define if an SNMP sensor will try again after a request fails. • **Retry (recommended)**: Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures. • **Do not retry**: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be put to error state earlier.
Overflow Values	Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks. • **Ignore overflow values (recommended)**: Ignore overflow values and do not include them in the monitoring data. • **Handle overflow values as valid results**: Regard all overflow values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
Zero Values	Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks.

© 2011 Paessler AG

SNMP Compatibility Options	
	• **Ignore zero values for delta sensors (recommended)**: Ignore zero values and do not include them in the monitoring data. • **Handle zero values as valid results for delta sensors**: Regard all zero values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
32-bit/64-bit Counters	Define which kind of traffic counters PRTG will search for on a device. • **Use 64-bit counters if available (recommended)**: The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices. • **Use 32-bit counters only**: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices. We recommend using the default value. If you experience problems, change this option.
Request Mode	Define which kind of request method PRTG uses for SNMP sensors. • **Use multi get (recommended)**: Bundle multiple SNMP requests into one request. • **Use single get**: Use one request for each SNMP value. This can increase compatibility with older devices. We recommend using the default value. If you experience problems, change this option.
Port Name Template	Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device/OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, **([port]) [ifalias]** is set as port name template, which will create a name such as *(001) Ethernet1*, for example. You can use any field names available at a certain OID of your device, among which are: • **[port]** • **[ifalias]** • **[ifname]** • **[ifindex]** • **[ifdescr]** Combine them as you like to obtain suitable sensor names. See the **More** section below for more information about SNMP sensor names.

HTTP Proxy Settings	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Please enter a string or leave the field empty.
Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current object will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.
Unusual Detection	
Unusual Detection	Define if unusual detection is enabled for sensors. You can set the behavior of unusual detection in the system settings. • **Enabled**: Enable unusual detection. Sensors will turn to orange color if unusual activity is detected. • **Disabled**: Disable unusual detection. To not use the orange sensor color.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to you needs. In an object's detail page, click on the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?
- http://www.paessler.com/knowledgebase/en/topic/313

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?
- http://www.paessler.com/knowledgebase/en/topic/7313

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?
- http://www.paessler.com/knowledgebase/en/topic/7363

© 2011 Paessler AG

6.5 Group Settings

On a group's overview page, click on the **Settings** tab to change settings.

Add Group

The **Add Group** dialog appears when adding a new group to a parent group. It only shows the setting fields that are imperative for creating the group. Therefore, you will not see all setting fields in this dialog. For example, the **Group Status** option is not available in this step.

You can change all settings in the group's **Settings** tab later.

Group Settings

The following settings are available in the **Settings** tab of every group. As you may not need all of these for every group, just regard those settings you really need, ignoring the others.

Note: This documentation does not refer to the setting of the special **Root** group. The settings available there differ from those described here.

We recommend defining as many settings as possible in the Root 166 group, so you can inherit them to all other objects further down in the tree hierarchy.

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Basic Group Settings	
Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Status	Choose if monitoring for this group is started or paused. • **Started**: Monitor this group. • **Paused**: Pause monitoring for this group. All sensors on all devices in this group will be paused until this setting is changed again.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like.
Priority	Select a priority for the group. This setting determines where the group will be placed in list views. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Group Type	
Sensor Management	Select which type of auto-discovery you would like to perform for this group. Choose between:

Group Type	
	• **Manual (no auto-discovery)**: Do not auto-discover any sensors, but only add sensors manually. • **Automatic device identification (standard, recommended)**: Use a small set of auto-discovery templates. This will scan your LAN and usually create a view standard sensors on your device. • **Automatic device identification (detailed, may create many sensors**: Use an extended set of auto-discovery templates. This will scan your LAN and usually create many sensors on your device. • **Automatic sensor creation using specific device templates**: Use specific auto-discovery templates only. Please select templates below. This will scan your LAN and add sensors defined in the template.
Device Template(s)	This option is only available if using specific device templates is enabled above. Choose one or more device templates from the list by adding a check mark in front of the respective template name. Choose from: ▪ **Cisco Device (Generic)** ▪ **DNS Server** ▪ **FTP Server** ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **HTTP Web Server** ▪ **Hyper V Host Server** ▪ **Linux/UNIX Device (SNMP or SSH enabled)** ▪ **LocalhostRDP** ▪ **Mail Server (Generic)** ▪ **Mail Server (MS Exchange 2003)** ▪ **Mail Server (MS Exchange 2007)** ▪ **Misc. Details** ▪ **Printer (HP)** ▪ **Server (Compaq/HP agents)** ▪ **Switch (Cisco Catalyst)** ▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)** ▪ **UNIX/Linux Device** ▪ **UPS (APC)** ▪ **VMware ESX Server** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)** ▪ **XEN Server**
Discovery Schedule	Define when the auto-discovery will be run. Choose between: • **Once**: Perform auto-discovery only once. New devices and sensors will be added once. You can run auto-discovery manually any time using an object's context menu 124. • **Hourly**: Perform auto-discovery for new devices and sensors every 60 minutes. *Note:* Please use this option with caution! Frequently executed auto-discoveries might cause performance issues, especially when large network segments are scanned every hour.

© 2011 Paessler AG

Device Template(s)	This option is only available if using specific device templates is enabled above. Choose one or more device templates from the list by adding a check mark in front of the respective template name. Choose from: ▪ **Cisco Device (Generic)** ▪ **DNS Server** ▪ **FTP Server** ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **HTTP Web Server** ▪ **Hyper V Host Server** ▪ **Linux/UNIX Device (SNMP or SSH enabled)** ▪ **LocalhostRDP** ▪ **Mail Server (Generic)** ▪ **Mail Server (MS Exchange 2003)** ▪ **Mail Server (MS Exchange 2007)** ▪ **Misc. Details** ▪ **Printer (HP)** ▪ **Server (Compaq/HP agents)** ▪ **Switch (Cisco Catalyst)** ▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)** ▪ **UNIX/Linux Device** ▪ **UPS (APC)** ▪ **VMware ESX Server** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)** ▪ **XEN Server**
	• **Daily**: Perform auto-discovery for new devices and sensors every 24 hours. The first auto-discovery will run immediately, all other discoveries will start on the time defined in the **Auto-Discovery Settings** section of the System Administration—System and Website 871 settings. • **Weekly**: Perform auto-discovery for new devices and sensors every 7 days. The first auto-discovery will run immediately, all other discoveries will start on the time defined in the **Auto-Discovery Settings** section of the System Administration—System and Website 871 settings.
IP Selection Method	Define how you want to define the IP range for auto-discovery. Choose between: ▪ **Class C base IP with start/end**: Define a class C address range. ▪ **List of individual IPs**: Enter individual IP addresses. ▪ **IP and subnet**: Enter an IP address and subnet mask. ▪ **IP with octet range**: Enter an IP address range for every IP octet individually. With this, you can define very customizable IP ranges. *Note:* Only subnets with up to 65,536 IP addresses can be discovered! If you define a range with a higher number of addresses, discovery will stop before it is completed.
IP Base	This field is only visible if Class C network detection is selected above. Enter a class C network as IP base for the auto-discovery. Enter the first three octets of an IPv4 IP address, for example, **192.168.0**

Device Template(s)	This option is only available if using specific device templates is enabled above. Choose one or more device templates from the list by adding a check mark in front of the respective template name. Choose from: ▪ **Cisco Device (Generic)** ▪ **DNS Server** ▪ **FTP Server** ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **HTTP Web Server** ▪ **Hyper V Host Server** ▪ **Linux/UNIX Device (SNMP or SSH enabled)** ▪ **LocalhostRDP** ▪ **Mail Server (Generic)** ▪ **Mail Server (MS Exchange 2003)** ▪ **Mail Server (MS Exchange 2007)** ▪ **Misc. Details** ▪ **Printer (HP)** ▪ **Server (Compaq/HP agents)** ▪ **Switch (Cisco Catalyst)** ▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)** ▪ **UNIX/Linux Device** ▪ **UPS (APC)** ▪ **VMware ESX Server** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)** ▪ **XEN Server**
IP Range Start	This field is only visible if Class C network detection is selected above. Enter the IP octet of the class C network specified above from which PRTG will start the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter **1** to discover from **192.168.0.1**.
IP Range End	This field is only visible if Class C network detection is selected above. Enter the IP octet of the class C network specified above at which PRTG will stop the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter **254** to discover up to **192.168.0.254**.
IP List	This field is only visible if the IP list option is selected above. Enter a list of IP addresses which the auto-discovery will scan. Enter each address in a separate line.
IP and Subnet	This field is only visible if the IP and subnet option is selected above. Enter an expression in the format **address/subnet**, e.g. *192.168.3.0/255.255.255.0*. You can also use the short form like *192.168.3.0/24* in this example. PRTG will scan the complete host range (without network and broadcast address) defined by the IP address and the subnet mask.

© 2011 Paessler AG

Device Template(s)	This option is only available if using specific device templates is enabled above. Choose one or more device templates from the list by adding a check mark in front of the respective template name. Choose from: ▪ **Cisco Device (Generic)** ▪ **DNS Server** ▪ **FTP Server** ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **HTTP Web Server** ▪ **Hyper V Host Server** ▪ **Linux/UNIX Device (SNMP or SSH enabled)** ▪ **LocalhostRDP** ▪ **Mail Server (Generic)** ▪ **Mail Server (MS Exchange 2003)** ▪ **Mail Server (MS Exchange 2007)** ▪ **Misc. Details** ▪ **Printer (HP)** ▪ **Server (Compaq/HP agents)** ▪ **Switch (Cisco Catalyst)** ▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)** ▪ **UNIX/Linux Device** ▪ **UPS (APC)** ▪ **VMware ESX Server** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)** ▪ **XEN Server**
IP with Octet Range	This field is only visible if the octet range option is selected above. Enter an expression in the format **a1.a2.a3.a4**, where *a1*, *a2*, *a3*, and *a4* are each a number between 0-255, or a range with two numbers and a hyphen like *1-127*. All permutations of all ranges are calculated, e.g. *10.0.1-10.1-100* results in 1,000 addresses that PRTG will scan during auto-discovery.
Name Resolution	Define how newly discovered devices will be monitored. This only affects *new* devices. The setting for existing devices will be kept. Choose between: • **Use DNS / WMI / SNMP names (recommended)**: Monitor newly discovered devices via their DNS, WMI, or SNMP names (if available). • **Use IP addresses**: Monitor newly discovered devices via their IP address. We recommend using the default value.
Device Rescan	Define if you want to rescan known devices. Choose between: • **Skip auto-discovery for known devices/IPs (recommended)**: Do not re-scan known devices or IP addresses, but only scan for new devices/IPs when auto-discovering. This can avoid re-creation of manually deleted sensors. PRTG will also avoid adding devices that are already included elsewhere in your configuration, e.g. in other groups.

Device Template(s)	This option is only available if using specific device templates is enabled above. Choose one or more device templates from the list by adding a check mark in front of the respective template name. Choose from: ▪ **Cisco Device (Generic)** ▪ **DNS Server** ▪ **FTP Server** ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **HTTP Web Server** ▪ **Hyper V Host Server** ▪ **Linux/UNIX Device (SNMP or SSH enabled)** ▪ **LocalhostRDP** ▪ **Mail Server (Generic)** ▪ **Mail Server (MS Exchange 2003)** ▪ **Mail Server (MS Exchange 2007)** ▪ **Misc. Details** ▪ **Printer (HP)** ▪ **Server (Compaq/HP agents)** ▪ **Switch (Cisco Catalyst)** ▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)** ▪ **UNIX/Linux Device** ▪ **UPS (APC)** ▪ **VMware ESX Server** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)** ▪ **XEN Server**
	• **Perform auto-discovery for known devices/IPs**: Re-scan known devices and IP addresses with every auto-discovery. This will re-create manually deleted sensors on existing devices. We recommend using the default value.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Location	
Location (for geo maps)	When using geo maps using Google's API 823 please enter a location in the first line. Objects will then be displayed on a geographical map with a flag, showing the current status using a color code similar to the sensor status icons 102 (green - yellow - red). You can enter a full postal address, city and country only, or latitude and longitude here. A minus sign (-) will hide an object from geo maps.

© 2011 Paessler AG

Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other sensors. If using a Windows local user account, please enter the computer name here. If using a Windows domain user account, please enter the domain name here.
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.
Credentials for Linux (SSH/WBEM) Systems	
Username	Enter a login name for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Password	Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **HTTP**: Use an unencrypted connection for WBEM. • **HTTPS**: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. • **Set manually**
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
Credentials for VMware/XEN Servers	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Choose between: • **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XEN servers. • **HTTP**: Use an unencrypted connection to VMware and XEN servers.
Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between:

Credentials for SNMP Devices	
	• **v1**: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. • **v2c**: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. • **v3**: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption. *Note for SNMP v3:* Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version **v1** or **v2c** are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: • **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication. • **SHA**: Use Secure Hash Algorithm (SHA) for authentication. Your device must be set to the same value.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. Your device must be set to the same value.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. Your device must be set to the same value.
Data Encryption Key (DES)	This setting is only visible if SNMP version v3 is enabled above. Enter a Data Encryption Standard (DES) key here. If you provide a key in this field, SNMP data packets will be enrypted using the DES encryption algorithm, providing increased security. Your device must be set to the same value. *Note:* If the key entered in this field does not match the key configured in the target SNMP device you will not get an error message! Please enter a string or leave the field empty.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
WMI Compatibility Options	
When experiencing problems while monitoring via Windows Management Instrumentation (WMI) sensors, you can set some compatibility options for trouble shooting.	

© 2011 Paessler AG

WMI Compatibility Options	
Timeout method	Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between: • **Use 1.5x scanning interval (recommended)**: Use a default of one and a half times the scanning interval set for the sensor (see below in this settings). • **Set manually**: Enter a timeout value manually. We recommend using the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.
Timeout value (sec.)	This field is only visible if manually timeout method is selected above. Specify the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value.
RPC server port	Specify the port which WMI uses for DCOM communication. We recommend using the default value. Only if you change this port on your system(s), please change it here.
SNMP Compatibility Options	
When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for trouble shooting.	
SNMP Delay (ms)	Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend using the default value. If you experience SNMP connection failures, please increase it.
Failed Requests	Define if an SNMP sensor will try again after a request fails. • **Retry (recommended)**: Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures. • **Do not retry**: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be put to error state earlier.
Overflow Values	Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks. • **Ignore overflow values (recommended)**: Ignore overflow values and do not include them in the monitoring data. • **Handle overflow values as valid results**: Regard all overflow values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
Zero Values	Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks. • **Ignore zero values for delta sensors (recommended)**: Ignore zero values and do not include them in the monitoring data. • **Handle zero values as valid results for delta sensors**: Regard all zero values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
32-bit/64-bit Counters	Define which kind of traffic counters PRTG will search for on a device.

SNMP Compatibility Options	
	• **Use 64-bit counters if available (recommended)**: The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices. • **Use 32-bit counters only**: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices. We recommend using the default value. If you experience problems, change this option.
Request Mode	Define which kind of request method PRTG uses for SNMP sensors. • **Use multi get (recommended)**: Bundle multiple SNMP requests into one request. • **Use single get**: Use one request for each SNMP value. This can increase compatibility with older devices. We recommend using the default value. If you experience problems, change this option.
Port Name Template	Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device/OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, **([port]) [ifalias]** is set as port name template, which will create a name such as *(001) Ethernet1*, for example. You can use any field names available at a certain OID of your device, among which are: • **[port]** • **[ifalias]** • **[ifname]** • **[ifindex]** • **[ifdescr]** Combine them as you like to obtain suitable sensor names. See the **More** section below for more information about SNMP sensor names.
HTTP Proxy Settings	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Please enter a string or leave the field empty.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current object will be dependent on.
Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.
Unusual Detection	
Unusual Detection	Define if unusual detection is enabled for sensors. You can set the behavior of unusual detection in the system settings. • **Enabled**: Enable unusual detection. Sensors will turn to orange color if unusual activity is detected. • **Disabled**: Disable unusual detection. To not use the orange sensor color.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to you needs. In an object's detail page, click on the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?
▪ http://www.paessler.com/knowledgebase/en/topic/313

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?
▪ http://www.paessler.com/knowledgebase/en/topic/7313

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?
▪ http://www.paessler.com/knowledgebase/en/topic/7363

© 2011 Paessler AG

6.6 Device Settings

On a device's details page, click on the **Settings** tab to change settings.

Add Device

The **Add Device** dialog appears when adding a new device to a group. It only shows the setting fields that are imperative for creating the device. Therefore, you will not see all setting fields in this dialog. For example, the **Device Status** option is not available in this step.

You can change all settings in the device's **Settings** tab later.

Device Settings

The following settings are available in the **Settings** tab of every device. As you may not need all of these for every device, just regard those settings you really need, ignoring the others.

We recommend defining as many settings as possible in the Root 166 group, so you can inherit them to all other objects further down in the tree hierarchy.

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Basic Device Settings	
Device Name	Enter a meaningful name to identify the device. The name will be shown by default in the sensor tree and in all alarms.
Status	Choose if monitoring for this device is started or paused. ▪ **Started**: Monitor this device. ▪ **Paused**: Pause monitoring for this device. All sensors on it will be paused until this setting is changed again.
IP Address/DNS Name	Enter the IP address or DNS name for the device. Most sensors created on this device will inherit this setting and they will try to connect to this address for monitoring. (However, some sensor types still have their own setting for IP address/DNS name.)
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Additional Device Information	
Device Icon	Choose a device icon from the list. It will be shown in the device tree. For information on how to add your custom icons, please see the link in the More 201 section below.
Service URL	Specify a URL you would like to open directly when choosing **Device Tools	Go To Service URL** from the device's context menu. For example, you can configure this option to call the address *http://www.example.com/service.html*. Enter a valid URL or leave the field empty.

Device Type	
Sensor Management	Select which type of auto-discovery you would like to perform for this device. Choose between: ▪ **Manual (no auto-discovery)**: Do not auto-discover any sensors, but only add sensors manually. ▪ **Automatic device identification (standard, recommended)**: Use a small set of auto-discovery templates. This will scan your LAN and usually create a view standard sensors on your device. ▪ **Automatic device identification (detailed, may create many sensors**: Use an extended set of auto-discovery templates. This will scan your LAN and usually create many sensors on your device. ▪ **Automatic sensor creation using specific device templates**: Use specific auto-discovery templates only. Please select templates below. This will scan your LAN and add sensors defined in the template.
Discovery Schedule	This option is only visible if one of the auto-discovery options is selected above. Define when the auto-discovery will be run. Choose between: ▪ **Once**: Perform auto-discovery only once. For existing devices, this will initiate a one-time sensor update for the current device. ▪ **Hourly**: Perform auto-discovery for new sensors every hour. ▪ **Daily**: Perform auto-discovery for new sensors every day. ▪ **Weekly**: Perform auto-discovery for new sensors every week.
Device Template(s)	This option is only visible if using specific device templates (last option) is enabled above. Please choose one or more templates by adding a check mark in front of the respective template name. These will be used for auto-discovery on the current device. Choose from: ▪ **Generic Device (PING only)** ▪ **Generic Device (SNMP-enabled, Detailed)** ▪ **Generic Device (SNMP-enabled)** ▪ **VMware ESX Server** ▪ **Hyper V Host Server** ▪ **Printer (HP)** ▪ **DNS Server** ▪ **FTP Server** ▪ **Server (Compaq/HP agents)** ▪ **HTTP Web Server** ▪ **Mail Server (MS Exchange 2007)** ▪ **Mail Server (MS Exchange 2003)** ▪ **Mail Server (Generic)**

© 2011 Paessler AG

Device Type	
	▪ **Switch (Cisco Catalyst)** ▪ **Switch (Cisco Generic)** ▪ **Switch (Cisco IOS Based)** ▪ **Switch (HP Procurve)** ▪ **UNIX/Linux Device** ▪ **UPS (APC)** ▪ **Windows (Detailed via WMI)** ▪ **Windows (via WMI)** ▪ **Windows IIS (via SNMP)**

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Location	
Location (for geo maps)	When using geo maps using Google's API 823 please enter a location in the first line. Objects will then be displayed on a geographical map with a flag, showing the current status using a color code similar to the sensor status icons 102 (green - yellow - red). You can enter a full postal address, city and country only, or latitude and longitude here. A minus sign (-) will hide an object from geo maps.
Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other sensors. If using a Windows local user account, please enter the computer name here. If using a Windows domain user account, please enter the domain name here.
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.
Credentials for Linux (SSH/WBEM) Systems	
Username	Enter a login name for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Password	Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **HTTP**: Use an unencrypted connection for WBEM. • **HTTPS**: Use an SSL-encrypted connection for WBEM.

Credentials for Linux (SSH/WBEM) Systems	
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: • **Set automatically (port 5988 or 5989)**: Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. • **Set manually**
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
Credentials for VMware/XEN Servers	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Choose between: • **HTTPS (recommended)**: Use an SSL-encrypted connection to VMware and XEN servers. • **HTTP**: Use an unencrypted connection to VMware and XEN servers.
Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between: • **v1**: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. • **v2c**: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. • **v3**: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption. *Note for SNMP v3:* Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version **v1** or **v2c** are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: • **MD5**: Use Message-Digest Algorithm 5 (MD5) for authentication. • **SHA**: Use Secure Hash Algorithm (SHA) for authentication. Your device must be set to the same value.

© 2011 Paessler AG

Credentials for SNMP Devices	
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. Your device must be set to the same value.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. Your device must be set to the same value.
Data Encryption Key (DES)	This setting is only visible if SNMP version v3 is enabled above. Enter a Data Encryption Standard (DES) key here. If you provide a key in this field, SNMP data packets will be enrypted using the DES encryption algorithm, providing increased security. Your device must be set to the same value. *Note:* If the key entered in this field does not match the key configured in the target SNMP device you will not get an error message! Please enter a string or leave the field empty.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
WMI Compatibility Options	
When experiencing problems while monitoring via Windows Management Instrumentation (WMI) sensors, you can set some compatibility options for trouble shooting.	
Timeout method	Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between: • **Use 1.5x scanning interval (recommended)**: Use a default of one and a half times the scanning interval set for the sensor (see below in this settings). • **Set manually**: Enter a timeout value manually. We recommend using the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.
Timeout value (sec.)	This field is only visible if manually timeout method is selected above. Specify the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value.
RPC server port	Specify the port which WMI uses for DCOM communication. We recommend using the default value. Only if you change this port on your system(s), please change it here.
SNMP Compatibility Options	
When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for trouble shooting.	
SNMP Delay (ms)	Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend using the default value. If you experience SNMP connection failures, please increase it.

SNMP Compatibility Options	
Failed Requests	Define if an SNMP sensor will try again after a request fails. • **Retry (recommended)**: Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures. • **Do not retry**: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be put to error state earlier.
Overflow Values	Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks. • **Ignore overflow values (recommended)**: Ignore overflow values and do not include them in the monitoring data. • **Handle overflow values as valid results**: Regard all overflow values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
Zero Values	Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks. • **Ignore zero values for delta sensors (recommended)**: Ignore zero values and do not include them in the monitoring data. • **Handle zero values as valid results for delta sensors**: Regard all zero values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
32-bit/64-bit Counters	Define which kind of traffic counters PRTG will search for on a device. • **Use 64-bit counters if available (recommended)**: The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices. • **Use 32-bit counters only**: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices. We recommend using the default value. If you experience problems, change this option.
Request Mode	Define which kind of request method PRTG uses for SNMP sensors. • **Use multi get (recommended)**: Bundle multiple SNMP requests into one request. • **Use single get**: Use one request for each SNMP value. This can increase compatibility with older devices. We recommend using the default value. If you experience problems, change this option.
Port Name Template	Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device/OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, **([port]) [ifalias]** is set as port name template, which will create a name such as *(001) Ethernet1*, for example. You can use any field names available at a certain OID of your device, among which are:

© 2011 Paessler AG

SNMP Compatibility Options	
	• **[port]** • **[ifalias]** • **[ifname]** • **[ifindex]** • **[ifdescr]** Combine them as you like to obtain suitable sensor names. See the **More** section below for more information about SNMP sensor names.
HTTP Proxy Settings	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Please enter a string or leave the field empty.
Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current object if its parent object is in a **Down** status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current object will be dependent on.
Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

© 2011 Paessler AG

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to you needs. In an object's detail page, click on the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, please see **Sensor Notifications Settings** 797 section.

Others

For more general information about settings, please see **Object Settings** 111 section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?
- http://www.paessler.com/knowledgebase/en/topic/313

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?
- http://www.paessler.com/knowledgebase/en/topic/7313

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?
- http://www.paessler.com/knowledgebase/en/topic/7363

6.7 Sensor Settings

There are more than 110 different sensor types available. In the **Add Sensor** dialog, all sensors are categorized into groups to help you quickly find what you need. Once you're familiar with the interface, you will probably enter the first letters of a sensor type's name into the **Search** field in the upper left corner and get to a sensor even faster.

Available Sensor Types

There is a dedicated manual section for every sensor with details about the available settings. For more information, please see List of Available Sensors 203 section.

Sensor Settings Overview

For information about sensor settings, please see the following sections:

- Sensor Settings 202
- List of Available Sensor Types 203

© 2011 Paessler AG

6.7.1 List of Available Sensor Types

This chapter simply lists all available sensors, sorted both by category and in alphabetical order.

- Common Sensors 203
- Bandwidth Monitoring Sensors 203
- Web Servers (HTTP) Sensors 203
- SNMP Sensors 204
- Windows/WMI Sensors 204
- Linux/Unix/OS X Sensors 204
- Virtual Servers Sensors 205
- SQL Servers Sensors 205
- File Servers Sensors 205
- Various Servers Sensors 206
- VoIP and QoS Sensors 206
- Custom Sensors 206
- All Sensors in Alphabetical Order 206
- More 209

Common Sensors

- Ping Sensor 452
- PORT Sensor 476
- HTTP Sensor 290
- SNMP Traffic Sensor 573
- WMI Network Card Sensor 740

Bandwidth Monitoring Sensors

- SNMP Traffic Sensor 573
- WMI Network Card Sensor 740
- Packet Sniffer (Content) Sensor 434
- Packet Sniffer (Header) Sensor 446
- NetFlow V5 Sensor 394
- NetFlow V9 Sensor 406
- sFlow V5 Sensor 504
- jFlow V5 Sensor 357

Web Servers (HTTP) Sensors

- HTTP Sensor 290
- HTTP Advanced Sensor 295
- HTTP Transaction Sensor 317
- HTTP Content Sensor 301
- HTTP Full Web Page Sensor 308
- HTTP SSL Certificate Expiry Sensor 312
- HTTP XML/REST Value Sensor 323

SNMP Sensors

- SNMP Linux Disk Free Sensor 558
- SNMP Linux Load Average Sensor 563
- SNMP Linux Meminfo Sensor 568
- SNMP Traffic Sensor 573
- SNMP Library Sensor 551
- SNMP Uptime Sensor 585
- SNMP Custom Sensor 540
- SNMP Custom String Sensor 546
- SNMP Trap Receiver Sensor 579

Windows/WMI Sensors

- WMI CPU Load Sensor 676
- WMI Memory Sensor 726
- WMI Uptime Sensor 772
- WMI Free Disk Space (Multi Drive) Sensor 711
- WMI Free Disk Space (Single Disk) Sensor 706
- WMI Network Card Sensor 740
- WMI Pagefile Sensor 744
- WMI Service Sensor 753
- WMI Share Sensor 758
- WMI Terminal Services (Windows XP/Vista/2003) Sensor 768
- WMI Terminal Services (Windows 2008) Sensor 768
- WMI Process Sensor 748
- WMI Event Log Sensor 686
- WMI File Sensor 701
- WMI Custom Sensor 680
- WMI Vital System Data Sensor 776
- Event Log (Windows API) Sensor 246
- Microsoft SQL Server 2005 Sensor 730
- Microsoft SQL Server 2008 Sensor 735
- WMI Exchange Server 2003 Sensor 693
- WMI Exchange Server 2007 Sensor 697
- WMI IIS 6.0 SMTP Received Sensor 718
- WMI IIS 6.0 SMTP Sent Sensor 722
- Windows Last Update Sensor 656
- Windows Logged In Users Sensor 661
- WMI Windows Version Sensor 781
- Windows Print Queue Sensor 671
- Active Directory Replication Errors Sensor 210
- Windows MSMQ Queue Length Sensor 666

Linux/Unix/OS X Sensors

- SSH Load Average Sensor 599
- SSH Meminfo Sensor 604
- SSH Disk Free Sensor 589
- SSH INodes Free Sensor 594
- SNMP Linux Load Average Sensor 563
- SNMP Linux Meminfo Sensor 568

© 2011 Paessler AG

- SNMP Linux Disk Free Sensor 558
- SNMP Traffic Sensor 573
- WBEM Custom Sensor 651

Virtual Servers Sensors

- VMware Host Server (SOAP) Sensor 642
- VMware Virtual Machine (SOAP) Sensor 646
- VMware Host Hardware (WBEM) 638
- Xen Virtual Machine Sensor 786
- Amazon CloudWatch Sensor 221
- Hyper-V Virtual Machine Sensor 333
- Hyper-V Virtual Storage Device Sensor 337
- Hyper-V Host Server Sensor 329
- Virtuozzo Container Disk Sensor 630
- Virtuozzo Container Network Sensor 634
- SSH VMWare ESX(i) Disk Sensor 609

Mail Servers Sensors

- SMTP Sensor 521
- POP3 Sensor 466
- SMTP&POP3 Round Trip Sensor 534
- IMAP Sensor 341
- SMTP&IMAP Round Trip Sensor 527
- WMI Exchange Server 2003 Sensor 693
- WMI Exchange Server 2007 Sensor 697
- WMI IIS 6.0 SMTP Sent Sensor 722
- WMI IIS 6.0 SMTP Received Sensor 718
- IP on DNS Blacklist Sensor 352
- POP3 Email Count Sensor 471

SQL Servers Sensors

- Microsoft SQL Sensor 380
- MySQL Sensor 387
- Oracle SQL Sensor 423
- ADO SQL Sensor 215
- WMI Microsoft SQL Server 2005 Sensor 730
- WMI Microsoft SQL Server 2008 Sensor 735

File Servers Sensors

- FTP Sensor 275
- TFTP Sensor 620
- WMI Free Disk Space (Multi Drive) Sensor 711
- WMI Free Disk Space (Single Disk) Sensor 706
- WMI File Sensor 701
- INI File Content Check Sensor 346
- Logfile Content Check Sensor 374
- FTP Server File Count Sensor 280
- Share Disk Free Sensor 516

- File Sensor 264
- Folder Sensor 269

Various Servers Sensors

- Ping Sensor 452
- Port Sensor 476
- NTP Sensor 418
- FTP Sensor 275
- FTP Server File Count Sensor 280
- TFTP Sensor 620
- DNS Sensor 241
- LDAP Sensor 369
- RDP (Remote Desktop) Sensor 492
- HDD Health Sensor 285
- RADIUS Sensor 487
- Syslog Receiver Sensor 614
- SNMP Trap Receiver Sensor 579
- DHCP Sensor 236
- Ping Jitter Sensor 456
- Traceroute Hop Count Sensor 625
- Ping with Delayed Up Sensor 461

VoIP and QoS Sensors

- QoS (Quality of Service) Sensor 481
- Cisco IP SLA Sensor 226

Custom Sensors

- SNMP Custom Sensor 540
- SNMP Custom String Sensor 546
- WMI Custom Sensor 680
- WBEM Custom Sensor 651
- EXE/Script Sensor 251
- EXE/Script Advanced Sensor 258
- Packet Sniffer (Custom) Sensor 440
- NetFlow V5 (Custom) Sensor 400
- NetFlow V9 (Custom) Sensor 412
- sFlow (Custom) Sensor 510
- jFlow V5 (Custom) Sensor 363
- Sensor Factory Sensor 497
- Pingdom Sensor 429

All Sensors in Alphabetical Order

- Active Directory Replication Errors Sensor 210
- ADO SQL Sensor 215
- Amazon CloudWatch Sensor 221
- Cisco IP SLA Sensor 226
- Cluster Probe Health Sensor 230
- Core/Probe Health Sensor 233

© 2011 Paessler AG

- DHCP Sensor 236
- DNS Sensor 241
- Event Log (Windows API) Sensor 246
- EXE/Script Sensor 251
- EXE/Script Advanced Sensor 258
- File Sensor 264
- Folder Sensor 269
- FTP Sensor 275
- FTP Server File Count Sensor 280
- HDD Health Sensor 285
- HTTP Sensor 290
- HTTP Advanced Sensor 295
- HTTP Content Sensor 301
- HTTP Full Web Page Sensor 308
- HTTP SSL Certificate Expiry Sensor 312
- HTTP Transaction Sensor 317
- HTTP XML/REST Value Sensor 323
- Hyper-V Host Server Sensor 329
- Hyper-V Virtual Machine Sensor 333
- Hyper-V Virtual Storage Device Sensor 337
- IMAP Sensor 341
- INI File Content Check Sensor 346
- IP on DNS Blacklist Sensor 352
- jFlow V5 Sensor 357
- jFlow V5 (Custom) Sensor 363
- LDAP Sensor 369
- Logfile Content Check Sensor 374
- Microsoft SQL Sensor 380
- MySQL Sensor 387
- NetFlow V5 Sensor 394
- NetFlow V5 (Custom) Sensor 400
- NetFlow V9 Sensor 406
- NetFlow V9 (Custom) Sensor 412
- NTP Sensor 418
- Oracle SQL Sensor 423
- Packet Sniffer (Content) Sensor 434
- Packet Sniffer (Custom) Sensor 440
- Packet Sniffer (Header) Sensor 446
- Ping Sensor 452
- Ping Jitter Sensor 456
- Ping with Delayed Up Sensor 461
- Pingdom Sensor 429
- POP3 Sensor 466
- POP3 Email Count Sensor 471
- Port Sensor 476
- QoS (Quality of Service) Sensor 481
- RADIUS Sensor 487
- RDP (Remote Desktop) Sensor 492
- Sensor Factory Sensor 497
- sFlow Sensor 504
- sFlow (Custom) Sensor 510
- Share Disk Free Sensor 516
- SMTP Sensor 521
- SMTP&IMAP Round Trip Sensor 527

- SMTP&POP3 Round Trip Sensor 534
- SNMP Custom Sensor 540
- SNMP Custom String Sensor 546
- SNMP Library Sensor 551
- SNMP Linux Disk Free Sensor 558
- SNMP Linux Load Average Sensor 563
- SNMP Linux Meminfo Sensor 568
- SNMP Traffic Sensor 573
- SNMP Trap Receiver Sensor 579
- SNMP Uptime Sensor 585
- SSH Disk Free Sensor 589
- SSH INodes Free Sensor 594
- SSH Load Average Sensor 599
- SSH Meminfo Sensor 604
- SSH VMWare ESX(i) Disk Sensor 609
- Syslog Receiver Sensor 614
- TFTP Sensor 620
- Traceroute Hop Count Sensor 625
- Virtuozzo Container Disk Sensor 630
- Virtuozzo Container Network Sensor 634
- VMware Host Hardware (WBEM) 638
- VMware Host Server (SOAP) Sensor 642
- VMware Virtual Machine (SOAP) Sensor 646
- WBEM Custom Sensor 651
- Windows Last Update Sensor 656
- Windows Logged In Users Sensor 661
- Windows MSMQ Queue Length Sensor 666
- Windows Print Queue Sensor 671
- WMI CPU Load Sensor 676
- WMI Custom Sensor 680
- WMI Event Log Sensor 686
- WMI Exchange Server 2003 Sensor 693
- WMI Exchange Server 2007 Sensor 697
- WMI File Sensor 701
- WMI Free Disk Space (Single Disk) Sensor 706
- WMI Free Disk Space (Multi Drive) Sensor 711
- WMI IIS 6.0 SMTP Received Sensor 718
- WMI IIS 6.0 SMTP Sent Sensor 722
- WMI Memory Sensor 726
- WMI Microsoft SQL Server 2005 Sensor 730
- WMI Microsoft SQL Server 2008 Sensor 735
- WMI Network Card Sensor 740
- WMI Pagefile Sensor 744
- WMI Process Sensor 748
- WMI Service Sensor 753
- WMI Share Sensor 758
- WMI Terminal Services (Windows 2008) Sensor 764
- WMI Terminal Services (Windows XP/Vista/2003) Sensor 768
- WMI Uptime Sensor 772
- WMI Vital System Data Sensor 776
- WMI Windows Version Sensor 781
- Xen Virtual Machine Sensor 786

© 2011 Paessler AG

More

Did not find what you're looking for? Have a look into the Additional Sensor Types (Custom Sensors) 790 section.

6.7.2 Active Directory Replication Errors Sensor

The Active Directory Replication Errors sensor uses its parent device's Windows credentials to find the first domain controller of the domain and retrieves a list of all available domain controllers. It then compares the returned lists and reports the number of errors found. Please make sure you enter valid domain credentials in the parent device's settings.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Active Directory Replication Errors Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Timeout (sec.)	Define a timeout in seconds for the entire process. If the reply takes longer than this value the request is aborted and an error message is triggered. Please enter an integer value.

© 2011 Paessler AG

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.3 ADO SQL Sensor

The ADO SQL sensor monitors a database using an ActiveX Data Objects (ADO) connection. It connects to the server and shows the response time. Additionally, it can read the number of records and a value.

Note: For security reasons, you can only create a sensor on a device for which Windows Credentials have been defined. With these credentials, the PRTG probe must be able to connect to the Windows domain. If you don't enter valid credentials, you will get an *Access denied* error message when scanning. For detailed information, please see More 219 section below.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

ADO SQL Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

ADO Specific Data	
Connectionstring	Enter the string that will be used to connect to the database. For example, such a string could be: *Provider=SQLOLEDB.1;Data Source=10.0.0.200\SQLEXPRESS;User ID=user;Password=userpass;Initial Catalog=Northwind*. For more information on how to build connection strings, please see More 219 section below.

Data	
SQL-Expression	Enter the SQL expression that will be queried from the database. For example, such an expression could be: *SELECT AVG(UnitPrice) FROM Products*. *Note:* When a cursor is returned (i.e. with a SELECT statement), only the first row of data will be processed.
Postprocessing	If the SQL expression returns a result set, please define if you want to further process it. Choose between: ▪ **Ignore result set**: Do not do anything with the data returned. ▪ **Process numerical result**: Regard the result set returned as integer or float. You can set the sensor to **Warning** or **Down** status for specific thresholds. Define below. ▪ **Process string result**: Regard the result set returned as a string. You can set the sensor to error for certain sub-strings contained or missing. Define below. ▪ **Monitor for changes**: Monitor if the result set has changed since last check. The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever a sensor value changes.
Condition "Warning"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a **Warning** status. Choose between: ▪ **none**: Do not set the sensor to **Warning** status for any condition. ▪ **equals**: Result set must be the same as the value provided below. ▪ **is above**: Result set must be above the value provided below. ▪ **lower than**: Result set must be below the value provided below. ▪ **does not equal**: Result set must be unequal to the value provided below. *Note:* This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings 792.
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor into a **Warning** status. Please enter an integer or float value.
Condition "Down"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a **Down** status. Choose between: ▪ **none**: Do not set the sensor to **Down** status for any condition. ▪ **equals**: Result set must be the same as the value provided below. ▪ **is above**: Result set must be above the value provided below. ▪ **lower than**: Result set must be below the value provided below. ▪ **does not equal**: Result set must be unequal to the value provided below. *Note:* This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings 792.
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor to a **Down** status. Please enter an integer value.

© 2011 Paessler AG

Postprocessing	If the SQL expression returns a result set, please define if you want to further process it. Choose between: ▪ **Ignore result set**: Do not do anything with the data returned. ▪ **Process numerical result**: Regard the result set returned as integer or float. You can set the sensor to **Warning** or **Down** status for specific thresholds. Define below. ▪ **Process string result**: Regard the result set returned as a string. You can set the sensor to error for certain sub-strings contained or missing. Define below. ▪ **Monitor for changes**: Monitor if the result set has changed since last check. The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever a sensor value changes.
Response must include	This field is only visible if string results is enabled above. Enter a string that must be part of the returned SQL string. If it is not, the sensor will be set to an error state. Please enter a string or leave the field empty.
Response must not include	This field is only visible if string results is enabled above. Enter a string that must not be part of the returned SQL string. If it is, the sensor will be set to an error state. Please enter a string or leave the field empty.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitoring (Almost) Any SQL Server Through ADO with PRTG Network Monitor
- http://www.paessler.com/knowledgebase/en/topic/2053

Knowledge Base: How do I correctly configure credentials for ADO SQL sensors?
- http://www.paessler.com/knowledgebase/en/topic/13103

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.4 Amazon CloudWatch Sensor

The Amazon CloudWatch sensor monitors performance of an Amazon EC2 computing instance using Amazon CloudWatch. The sensor shows CPU uitilization, network load in and out, and disk read and write speed.

Note: The CloudWatch option must be enabled for the instance you want to monitor (you can do this e.g. using Amazon's AWS console).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Amazon CloudWatch Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Amazon CloudWatch Specific	
Timeout	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Period (Interval)	Define in what granularity you want to receive datapoints from CloudWatch. Choose between: • **1 Minute** • **2 Minutes** • **5 Minutes** • **10 Minutes**
AWS Access Key ID	Enter your access key. You can obtain in from aws.amazon.com.
AWS Secret Access Key	Enter your secret access key. You can obtain in from aws.amazon.com.
Instance	Enter the ID of the instance this sensor will monitor.
Region	Select the region in which the instance to be monitored is running. Choose between: • **US-West (USA)** • **US-East (USA)** • **EU-West (Europe)** • **AP-Southeast (Asia Pacific)**

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Note: For Amazon CloudWatch sensors, the scanning interval cannot be inherited. Please use the individual settings of the sensor to define the interval in which data is received.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.5 Cisco IP SLA Sensor

The Cisco IP SLA sensor monitors Voice over IP (VoIP) network parameters using IP Service Level Agreement (SLA) from Cisco via Simple Network Management Protocol (SNMP). It shows different aspects provided by the queried device.

For a general introduction to the technology behind Quality of Service monitoring, please see Monitoring Quality of Service 947 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

IP SLA Specific	
IP SLAs	A list of possible SLA types is shown. The list options depend on the configuration of the queried device. If you're missing a type here, please check your device's configuration. To add an SLA type to your monitoring, add a check mark in front of the respective line. For each selection one SLA sensor will be created. They are named automatically. PRTG can support the following operations: ▪ **echo** ▪ **pathEcho** ▪ **fileIO** ▪ **script** ▪ **udpEcho** ▪ **tcpConnect** ▪ **http** ▪ **dns** ▪ **jitter** ▪ **dlsw** ▪ **dhcp** ▪ **ftp** ▪ **path-jitter** * *Note:* Packet Loss values are summarized, but have no explicit channel for Source-->Destination or Destination-->Source values ** Available for PRTG v8.3 or later*

Cisco IP SLA Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

© 2011 Paessler AG

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

IP SLA Specific	
ID	These fields show SLA specific settings provided by the queried SLA device. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Type	
Name (Tag)	
Owner	
Frequency	

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.6 Cluster Probe Health Sensor

The Cluster Probe Health sensor is a system device indicating PRTG's own system health status. It is created automatically with a PRTG cluster installation and cannot be deleted. It measures various internal system parameters of the cluster system and the probe's internal processes and then computes a resulting value. Frequent or repeated health values below 100 % should be investigated, please check the sensor's channels for details.

Cluster Probe Health Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

© 2011 Paessler AG

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.7 Core/Probe Health Sensor

The Core/Probe Health sensor is a system device indicating PRTG's own system health status. It is created automatically with your PRTG installation and cannot be deleted. It measures various internal system parameters of the probe system hardware and the probe's internal processes and then computes a resulting value. Frequent or repeated health values below 100 % should be investigated, please check the sensor's channels for details.

For detailed information on the different channels, please activate the help box when in the sensor's **Overview** tab. A box will appear at the end of the page, explaining the meaning of the different channels.

Core/Probe Health Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the **System Administration—User Groups** 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

© 2011 Paessler AG

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.8 DHCP Sensor

The DHCP sensor monitors a Dynamic Host Configuration Protocol (DHCP) server. It sends a broadcast message to the network and waits for a DHCP server to respond. If a server responds the sensor shows both the address of the server and the offered IP in the sensor's **Message** field. The sensor's channels include response time (msec) and the lease time given by the server.

This sensor can be set up on a Probe Device only!

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

DHCP Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

DHCP Specific	
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor.

© 2011 Paessler AG

Sensor Display	
	▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.9 DNS Sensor

The DNS sensor monitors a Domain Name Service (DNS) server. It resolves a domain name and compares it to a given IP address. The sensor shows the response time and goes to an error state if the DNS server does not resolve a given domain name correctly.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

DNS Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

DNS Specific	
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Enter the number of the port the sensor will try to connect to. This must be the port the sensor's parent device is running the DNS service on. We recommend using the default value.
Domain	Enter the domain name that will be resolved by the sensor using the Domain Name Service (DNS) server specified in the sensor's parent device's settings. You can enter an internet domain name here (for example, *example.com*), or a DNS name in your internal network (such as *computer-xyz*); depending on the type of DNS server you will monitor.

DNS Specific	
IP Address	Enter the IP address of the domain specified above. The sensor will compare this value to the IP address resolved for the given domain name. If the two values do not match an error message will be triggered.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.10 Event Log (Windows API) Sensor

The Event Log (Windows API) sensor monitors Event Log entries using Windows Application Programming Interface (API). It shows the number of new records per second (speed).

Windows API Event Log specific	
Log file	Specify the log file the sensor will monitor. The Windows event log provides several different log files. A drop down list specific to your system is shown. Please select a log file from the list. Choose between: • **Application** • **System** • **Security** • **Directory Service** • **DNS Server** • **File Replication Service**

Filter Event Log Entries	
Filter by Source	Filter all received events for a certain event source. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • **Off**: Do not filter by event source. • **On**: Enable filtering by event source.
Match String (Event Source)	This field is only visible if filtering is enabled above. Enter a source from which the events are to come from. Only events from a source matching this string will be regarded, others ignored. You can also use the percent sign (%) as placeholder for any or no character (as known from the asterisk sign (*) in Windows search) in combination with a substring. For example, you can enter **%RAS%** for any event source containing the string **RAS**. Please enter a string.
Filter by ID	Filter all received events for a certain event ID. If enabled, only messages matching the defined value(s) will be considered by the sensor. Choose between: • **Off**: Do not filter by event ID. • **On**: Enable filtering by event ID.
Match Value (Event ID)	This field is only visible if filtering is enabled above. Enter one or more event IDs (comma separated) from which the events are to come from. Only events with an ID matching one of the values will be regarded. Please enter one integer value or more comma separated integer values.
Filter by Category	Filter all received events for a certain event category. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • **Off**: Do not filter by event category. • **On**: Enable filtering by event category.

© 2011 Paessler AG

Filter Event Log Entries	
Match String (Event Category)	This field is only visible if filtering is enabled above. Enter a category which the events are to have. Only events with a category matching this string will be regarded. You can also use the percent sign (%) as placeholder for any or no character (as known from the asterisk sign (*) in Windows search) in combination with a substring. For example, you can enter **%N%** for any event category containing the character **N**. Please enter a string.
Filter by Event User	Filter all received events for a certain event user. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • **Off**: Do not filter by event user. • **On**: Enable filtering by event user.
Match String (Event User)	This field is only visible if filtering is enabled above. Enter a user name which the event are to be assigned to. Only events with a user name matching this string will be regarded. You can also use the percent sign (%) as placeholder for any or no character (as known from the asterisk sign (*) in Windows search) in combination with a substring. For example, you can enter **A%** for any user name starting with the character **A**. Please enter a string.
Filter by Event Computer	Filter all received events for a certain event computer. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • **Off**: Do not filter by event computer. • **On**: Enable filtering by event computer.
Match String (Event Computer)	This field is only visible if filtering is enabled above. Enter a computer name which the events are to be assigned to. Only events with a computer name matching this string will be regarded. You can also use the percent sign (%) as placeholder for any or no character (as known from the asterisk sign (*) in Windows search) in combination with a substring. Please enter a string.
Filter by Event Message	Filter all received events for a certain event message. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • **Off**: Do not filter by event message. • **On**: Enable filtering by event message.
Match String (Event Message)	This field is only visible if filtering is enabled above. Enter a message which the event must contain. Only events with a message matching this string will be regarded. You can use the percent sign (%) as placeholder for any or no character (as known from the asterisk sign (*) in Windows search) in combination with a substring here. Please enter a string.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.11 EXE/Script Sensor

The EXE/Script sensor runs an executable file (EXE, DLL) or a script (batch file, VBScript, Powershell) on the computer running the local or remote probe. This option is provided as part of PRTG's Application Programming Interface (API). The sensor shows the execution time, and can show one value returned by the executable file or script (in one channel only). For details about the return value format please see the Application Programming Interface (API) definition linked in the **More** 256 section below.

Note: The executable or script file must be stored on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.

Note: If you want to execute a custom Windows Management Instrumentation Query Language (WQL) script, please use the **WMI Custom Sensor** 680.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Exe/Script Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
EXE/Script	Select an executable file from the list. It will be executed with every scanning interval. In this list, files in the corresponding **/Custom Sensors/EXE** sub-directory of the probe system's PRTG installation are shown. In order for the files to appear in this list, please store them into this folder. Store files ending in BAT, CMD, DLL, EXE, PS1, and VBS. In order for the sensor to show the right status, your files must use the right format for the returned values. For detailed information on how to build custom sensors, please see the API documentation (Application Programming Interface (API) Definition 979). *Note:* Please do not use the folder *\Custom Sensors\Powershell Scripts* to store your files. This remnant from previous software versions is not used any more and may usually be deleted. *Note:* When using custom sensors on the **Cluster Probe**, please copy your files to every cluster node installation.
Parameters	If your executable or script file catches command line parameters, you can define them here. Placeholders can be used as well. For a full list of all placeholders please see the API documentation (Application Programming Interface (API) Definition 979). Please enter a string or leave the field empty.
Environment	Choose if PRTG's command line parameters will also be available as environment parameters. ▪ **Default Environment**: Do not provide PRTG placeholders' values in the environment. Choose this secure option if you're not sure. ▪ **Set placeholders as environment values**: From within your executable or script, the values of PRTG's command line parameters will be available via environment variables. For example, you can then read and use the current *host* value of the PRTG device this EXE/script sensor is created on from within your script. This option can mean a security risk, because also credentials are provided in several variables. For a full list of all available variables please see the API documentation (Application Programming Interface (API) Definition 979).
Security Context	Define the Windows user account that will be used to run the executable or script file. Choose between: • **Use security context of probe service**: Run the selected file under the same Windows user account the probe is running on. By default, this is the Windows system user account (if not manually changed). • **Use Windows credentials of parent device**: Use the Windows user account defined in the settings of the parent device this sensor is created on. Please go to sensor's parent device's settings to change these Windows credentials.
Mutex Name	Define any desired mutex name for the process. All EXE/Script sensors having the same mutex name will be executed serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running simultaneously. For links to more information, please see the More 256 section below. Please enter a string or leave the field empty.

© 2011 Paessler AG

Sensor Settings	
Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the external process is killed and an error message is triggered.
Value Type	Define what kind of values your executable or script file gives back. Choose between: • **Integer**: An integer is expected as return value. If the script gives back a float, PRTG will display the value **0**. • **Float:** A float is expected as return value, with a dot (.) between pre-decimal position and decimal places. In this setting, the sensor will also display integer values unless they don't produce a buffer overflow. The sensor cannot handle string values. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Channel Name	Enter a name for the channel in which the returned values will be shown. This is for display purposes only. Please enter a string.
Unit String	Enter a string describing the unit of the returned values. This is for display purposes only. Please enter a string.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change. • **Trigger 'On Change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.
EXE Result	Define what will be done with the result the executable file gives back. Choose between: • **Discard EXE result**: Do not store the requested web page. • **Write EXE result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the script to the "Logs (System)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **More** 256 section below.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

More

- Application Programming Interface (API) Definition 979
- Additional Sensor Types (Custom Sensors) 790

Paessler Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?
- http://www.paessler.com/knowledgebase/en/topic/6673

Paessler Knowledge Base: How and Where Does PRTG Store its Data?
- http://www.paessler.com/knowledgebase/en/topic/463

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

© 2011 Paessler AG

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.12 EXE/Script Advanced Sensor

The EXE/Script Advanced sensor runs an executable file (EXE, DLL) or a script (batch file, VBScript, Powershell) on the computer running the local or remote probe. This option is provided as part of PRTG's Application Programming Interface (API). The sensor shows the execution time, and can show values returned by the executable file or script in multiple channels. The return value of this sensor must be valid XML. For details about the return value format please see the Application Programming Interface (API) definition linked in the **More** 262 section below.

Note: The executable or script file must be stored on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.

Note: If you want to execute a custom Windows Management Instrumentation Query Language (WQL) script, please use the **WMI Custom Sensor** 680.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Exe/Script Advanced Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

Sensor Settings	
EXE/Script	Select an executable file from the list. It will be executed with every scanning interval. In this list, files in the corresponding **/Custom Sensors/EXEXML** sub-directory of the probe system's PRTG installation are shown. In order for the files to appear in this list, please store them into this folder. Store files ending in BAT, CMD, DLL, EXE, PS1, and VBS. In order for the sensor to show the right status, your files must use the right format for the returned values. For detailed information on how to build custom sensors, please see the API documentation (Application Programming Interface (API) Definition 979). *Note:* Please do not use the folder *\Custom Sensors\Powershell Scripts* to store your files. This remnant from previous software versions is not used any more and may usually be deleted. *Note:* When using custom sensors on the **Cluster Probe**, please copy your files to every cluster node installation.
Parameters	If your executable or script file catches command line parameters, you can define them here. Placeholders can be used as well. For a full list of all placeholders please see the API documentation (Application Programming Interface (API) Definition 979). Please enter a string or leave the field empty.
Environment	Choose if PRTG's command line parameters will also be available as environment parameters. ▪ **Default Environment**: Do not provide PRTG placeholders' values in the environment. Choose this secure option if you're not sure. ▪ **Set placeholders as environment values**: From within your executable or script, the values of PRTG's command line parameters will be available via environment variables. For example, you can then read and use the current *host* value of the PRTG device this EXE/script sensor is created on from within your script. This option can mean a security risk, because also credentials are provided in several variables. For a full list of all available variables please see the API documentation (Application Programming Interface (API) Definition 979).
Security Context	Define the Windows user account that will be used to run the executable or script file. Choose between: • **Use security context of probe service**: Run the selected file under the same Windows user account the probe is running on. By default, this is the Windows system user account (if not manually changed). • **Use Windows credentials of parent device**: Use the Windows user account defined in the settings of the parent device this sensor is created on. Please go to sensor's parent device's settings to change these Windows credentials.
Mutex Name	Define any desired mutex name for the process. All EXE/Script sensors having the same mutex name will be executed serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running simultaneously. For links to more information, please see the More 262 section below. Please enter a string or leave the field empty.

Sensor Settings	
Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the external process is killed and an error message is triggered.
EXE Result	Define what will be done with the results the executable file gives back. Choose between: • **Discard EXE result**: Do not store the requested web page. • **Write EXE result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the script to the "Logs (System)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see More 262 section below.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Note: The **Stack Unit** option for stacking graphs will only work if you explicitly define the same *<unit>* for at least two channels. For detailed information about sensor settings please see the API documentation (Application Programming Interface (API) Definition 979).

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

More

- Application Programming Interface (API) Definition 979
- Additional Sensor Types (Custom Sensors) 790

Paessler Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?
- http://www.paessler.com/knowledgebase/en/topic/6673

Paessler Knowledge Base: How and Where Does PRTG Store its Data?
- http://www.paessler.com/knowledgebase/en/topic/463

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

© 2011 Paessler AG

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.13 File Sensor

The File sensor monitors a folder using Server Message Block (SMB). You can monitor file content and file time stamp changes. It shows the file size, and a last modified value in days and hours.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

File Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

Sensor Specific	
File Name	Enter the full path to the file this sensor will monitor. If the file is located on a network device use the Uniform Naming Convention (UNC) path *without* the server part (you would only enter *share\folder\file.txt*). The server part (*\\server*) is taken from this sensor's parent device's settings. Please enter a valid path and file name.
Monitor File Content	Specify if the sensor will send a change notification when the content of the file changes (based on a checksum). Choose between: • **Ignore changes (default)**: Changes to the file will not trigger a change notification. • **Trigger 'On Change' notification**: The sensor will trigger a change notification if the file's checksum has changed.
Monitor file time stamp	Specify if the sensor will send a change notification when the content of the file's time stamp changes. Choose between: • **Ignore changes (default)**: Changes to the time stamp will not trigger a change notification. • **Trigger 'On Change' notification**: The sensor will trigger a change notification if a file's time stamp has changed.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.14 Folder Sensor

The Folder sensor monitors a folder using Server Message Block (SMB). You can monitor file changes and specified file ages. It shows the folder size, file count, and oldest and newest file value in days and hours.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Folder Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Folder Monitor	
Folder Name	Enter the folder this sensor will monitor. Enter the path to the folder. If the folder is located on a network device use the Uniform Naming Convention (UNC) path *without* the server part (you would only enter *share\folder*). The server part (*\\server*) is taken from this sensor's parent device's settings. Please enter a valid path name.
Sub-Folder Recursion	Specify if subfolders will be included in the monitoring. Choose between: • **Do not recurse sub-folders**: Only monitor the folder specified above; do not monitor its subfolders. • **Monitor the folder and its sub-folders (use with caution!)**: Monitor the folder specified above and all of its subfolders. *Note:* Recursing sub-folders in large directories with a high number of branches may evoke timeout errors or performance issues.
Monitor folder changes	Specify if the sensor will send a change notification when the content of the folder changes. Choose between: • **Ignore changes (default)**: Changes to the folder will not trigger a change notification. • **Trigger 'On Change' notification**: The sensor will trigger a change notification if a file changes its timestamp or filename, or if there are new or deleted files.
Check of File Ages	Specify if the sensor will monitor the folder for certain file ages. Choose between: • **Don't check**: Do not check for the age of the files in the specified folder (s). • **Show Warning if older**: Set the sensor to warning status if one of the files in the specified folder is older than... • **Show Error if older**: Set the sensor to error status if one of the files in the specified folder is older than... • **Show Warning if younger**: Set the sensor to warning status if one of the files in the specified folder is younger than... • **Show Error if younger**: Set the sensor to error status if one of the files in the specified folder is younger than...
File Age Limit	This field is only visible if a file age check is enabled above. Enter the age of a file in the folder that will trigger the sensor's status change if undershot respectively overrun. Please enter an integer value. The value will be interpreted as days, hours, or minutes; according to your setting below.
File Age Limit Unit	This field is only visible if a file age check is enabled above. Specify the unit for the file age below. Choose between: • **In days**: You will enter a number of days below. • **In hours**: You will enter a number of hours below. • **In minutes**: You will enter a number of minutes below.

© 2011 Paessler AG

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.15 FTP Sensor

The FTP sensor monitors file servers using File Transfer Protocol (FTP) and FTP over SSL (FTPS). It shows the response time.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

FTP Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

FTP Settings	
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Enter the number of the port the sensor will try to connect to. For non-secure connections usually port 21 is used; usually port 990 for implicit secure connections. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
FTP Mode	Specify which ftp mode will be used for the connection. Choose between: • **Use active mode (default)** • **Use passive mode** We recommend using the default value. If you do not get a connection, please try the passive mode.

Authentication	
Username	Enter a username for the FTP login. Please enter a string or leave the field empty.
Password	Enter a password for the FTP login. Please enter a string or leave the field empty.
TLS (Transport-Level-Security)	Specifiy if an encryption will be used for the connection. Choose between: • **Don't use SSL (Basic FTP, recommended)** • **Use SSL (FTP over SSL/FTPS)** In most cases, you will use basic FTP without encryption.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.16 FTP Server File Count Sensor

The FTP Server File Count sensor logs in to an FTP server and returns the number of files available in the directory listing.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Channel Name	Enter a name for the channel in which the returned values will be shown. This is for display purposes only. Please enter a string.

FTP Server File Count Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
FTP URL	Enter the URL to check (this sensor does *not* use the **IP Address/DNS value** of the parent device).

© 2011 Paessler AG

Sensor Settings	
Username	Define the username for the login. Please enter a string.
Password	Define the password for the login. Please enter a string.
File Extension Include Filter	If you want to count files with certain file extensions only, define one or more extensions, separated by comma. Only matching files will be counted. You can enter the extension with or without dot. For example, enter *.exe,txt* to only count *.EXE and *.TXT files. Please enter a string or leave the field empty.
File Extension Exclude Filter	If you want to explicitly exclude files with certain file extensions from the file count, define one or more extensions, separated by comma. Only non-matching files will be counted. You can enter the extension with or without dot. For example, enter *.exe,txt* to not count *.EXE and *.TXT files, but only files with other extensions. *Note:* The exclude filter overrules the include filter. Please enter a string or leave the field empty.
Timeout (sec.)	Define a timeout in seconds for the entire process. If the reply takes longer than this value the request is aborted and an error message is triggered. Please enter an integer value.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change. • **Trigger 'change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.17 HDD Health Sensor

Monitors the health of IDE disk drives using Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T./SMART). This is built into most modern IDE hard disk drives.

It can show the following channels: Temperature, Read Error Rate, Throughput Performance, Spin-Up Time, Start/Stop Count, Reallocated Sectors Count, Power On Count, Spin Retry Count, Recalibration Retries, Device Power Cycle Count, Soft Read Error Rate, High Fly Writes (WDC), Reallocation Event Count, Current Pending Sector Count, Uncorrectable Sector Count, Off-Track Error Rate, and Downtime.

This sensor can be set up on a Probe Device only!

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

SMART Specific	
IDE Devices	Please select one or more hard disks from the list by adding a check mark in front of the respective line. For every HDD one sensor will be created. Names are chosen automatically and can be changed later in the sensor's settings. The items shown in the list are specific to the probe system you're creating the sensor on.

HDD Health Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.

Basic Sensor Settings	
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SMART Specific	
Serial No.	Shows the serial number of the monitored disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the monitored disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Size (GB)	Shows the size in Gigabyte of the monitored disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Temperature threshold	Shows the temperature threshold value stored in the monitored disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

© 2011 Paessler AG

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.18 HTTP Sensor

The HTTP sensor monitors a web server using Hypertext Transfer Protocol (HTTP). It shows the loading time. This is the easiest way to monitor if a website (or a specific website element) is reachable.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

HTTP Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

HTTP Specific	
Timeout (sec.)	Enter a timeout in seconds for the HTTP request. If the reply takes longer than this value the request is aborted and an error message is triggered.
URL	Please enter the URL the sensor will connect to. This address can be independent from the **IP address/DNS name** setting of the device this sensor is created on. PRTG uses a smart URL replacements which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.
Request Method	The request method determines how the given URL is requested. • **GET**: Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page. • **POST**: Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Postdata** field below.

© 2011 Paessler AG

HTTP Specific	
	• **HEAD**: Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.
Postdata	This field is only active when POST is selected in the **Request Method** setting above. Please enter the data part for the post request here. *Note:* No XML is allowed here!
SSL Method	This setting is relevant only when using https in the **URL** field. We recommend using the default value. If you experience connection problems, please select another SSL method from the drop down menu.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

HTTP Proxy Settings	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Please enter a string or leave the field empty.
Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either *http:///* or *https:///* or even a simple slash */* as equivalent for *http:///*). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** *www.example.com* and you put a HTTP sensor on it with the value *https:///* in the URL field, PRTG will automatically create the URL *https://www.example.com/* from that. Similarly, if you create a HTTP sensor on the same device using the value */help* in the URL field, PRTG will automatically create and monitor the URL *http://www.example.com/help*

Note: Smart URL replacement does not work for sensors running on the "Probe Device".)

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.19 HTTP Advanced Sensor

The HTTP Advanced sensor monitors the source code of a web page using Hypertext Transfer Protocol (HTTP). It supports authentication, content checks, and other advanced parameters. It shows the loading time, bytes received, download bandwidth (speed), and time to first byte.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

HTTP Advanced Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

HTTP Specific	
Timeout (sec.)	Enter a timeout in seconds for the HTTP request. If the reply takes longer than this value the request is aborted and an error message is triggered.
URL	Please enter the URL the sensor will connect to. This address can be independent from the **IP address/DNS name** setting of the device this sensor is created on. PRTG uses a smart URL replacements which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.
Request Method	The request method determines how the given URL is requested. • **GET**: Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page. • **POST**: Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Postdata** field below.

HTTP Specific	
	• **HEAD**: Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.
Postdata	This field is only active when POST is selected in the **Request Method** setting above. Please enter the data part for the post request here. *Note:* No XML is allowed here!
SSL Method	This setting is relevant only when using https in the **URL** field. We recommend using the default value. If you experience connection problems, please select another SSL method from the drop down menu.

Advanced Sensor Data	
Content Changes	Define what shall be done in case the content of the monitored web page changes. You can choose between: • **Ignore changes**: No action will be taken on change. • **Trigger 'change' notification**: The sensor will send an internal message indicating that the web page content has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the web page content changes.
Response must include	Define which string must be part of the source code at the given URL. If the data does not include this string, the sensor will be set to an error state. Please enter a string or leave the field empty.
Response must not include	Define which string must not be part of the source code at the given URL. If the data does include this string, the sensor will be set to an error state. Please enter a string or leave the field empty.
Limit Download (kb)	Enter a maximum amount of data that will be transferred per every single request. If you set content checks below, please be aware that only the content downloaded within this limit can be checked for certain search expressions.
Result Handling	Define what will be done with the web page loaded at the given URL. Choose between: • **Discard HTML result**: Do not store the requested web page. • **Store latest HTML result**: Store the last result of the requested web page to the "Logs (System)" directory (on the Master node, if in a cluster). This is for debugging purposes, especially in combination with content checks. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **More** 300 section below.

© 2011 Paessler AG

Note: This sensor loads the source code at the given URL. If you set up a content check, only this source code is checked for the keywords. The code is not necessarily identical to the one used to display the page when opening the same URL in a web browser, as there may be a reload configured or certain information may be inserted after loading, e.g. via Javascript. PRTG does not follow links to embedded objects nor does it execute scripts. Only the first page at the given URL is loaded and checked against the expressions configured. For debugging, please use the **Result** option to write the source code file to disk and look up what exactly PRTG 'sees' when calling the URL.

Authentication	
User	If the URL is protected and needs authentication, enter a username here. Please enter a string or leave the field empty.
Password	If the URL is protected and needs authentication, enter a password here. Please enter a string or leave the field empty.
Authentication Method	If you have entered credentials above, please select the authentication method the given URL is protected with. Choose between: • **Basic access authentication (HTTP)**: Use simple HTTP authentication. This is suitable for most cases. • **Windows NT LAN Manager (NTLM)**: Use the Microsoft NTLM protocol for authentication. This is sometimes used in Intranets for single sign-on. We recommend using the default value.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

HTTP Proxy Settings	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Please enter a string or leave the field empty.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either *http:///* or *https:///* or even a simple slash */* as equivalent for *http:///*). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** *www.example.com* and you put a HTTP sensor on it with the value *https:///* in the URL field, PRTG will automatically create the URL *https://www.example.com/* from that. Similarly, if you create a HTTP sensor on the same device using the value */help* in the URL field, PRTG will automatically create and monitor the URL *http://www.example.com/help*

Note: Smart URL replacement does not work for sensors running on the "Probe Device".)

More

Knowledge Base article: How and Where Does PRTG Store its Data?

- http://www.paessler.com/knowledgebase/en/topic/463

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.20 HTTP Content Sensor

The HTTP Content sensor monitors a numerical value returned by a Hypertext Transfer Protocol (HTTP) request. In the returned HTML page, each value must be placed between square brackets [ ].

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

HTTP Content Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

HTTP Specific	
Timeout (sec.)	Enter a timeout in seconds for the HTTP request. If the reply takes longer than this value the request is aborted and an error message is triggered.
URL	Please enter the URL the sensor will connect to. This address can be independent from the **IP address/DNS name** setting of the device this sensor is created on. PRTG uses a smart URL replacements which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.
Request Method	The request method determines how the given URL is requested. • **GET**: Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page. • **POST**: Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Postdata** field below.

HTTP Specific	
	• **HEAD**: Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.
Postdata	This field is only active when POST is selected in the **Request Method** setting above. Please enter the data part for the post request here. *Note:* No XML is allowed here!
SSL Method	This setting is relevant only when using https in the **URL** field. We recommend using the default value. If you experience connection problems, please select another SSL method from the drop down menu.

HTTP Specific	
Timeout (sec.)	Enter a timeout in seconds for the HTTP request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Script URL	Please enter the URL the sensor will connect to. This address can be independent from the **IP address/DNS name** setting of the device this sensor is created on. PRTG uses a smart URL replacements which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.
Value Type	Define what kind of values your HTML file gives back. Choose between: • **Integer**: An integer is expected as return value. • **Float:** A float is expected as return value, with a dot (.) between pre-decimal position and decimal places. In this setting, the sensor will also display integer values unless they don't produce a buffer overflow. The sensor cannot handle string values. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Number of channels	Define how many values your HTML file gives back. Each value will be handled in its own sensor channel. Each value must be placed between square brackets [ ]. Enter the number of bracket-value pairs that will be returned at the defined URL. Do not enter a number less than the number of values returned. Otherwise you will get an error message.
SSL-Method	This setting is only relevant when using a **https** protocol in the **Script URL**. Select the SSL method that will be used when connecting to the URL. We recommend using the default value. Only if you experience connection problems, try another setting.

Advanced Sensor Data	
Content changes	Define what shall be done in case the content of the monitored web page changes. You can choose between:

© 2011 Paessler AG

Advanced Sensor Data	
	• **Ignore changes**: No action will be taken on change. • **Trigger 'change' notification**: The sensor will send an internal message indicating that the web page content has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the web page content changes.

Example

At the URL *http://www.example.com/status.html* a PHP script is giving back the current system status in a simple HTML page, as follows:

```
<html>
 <body>
  Description: Script gives back current status of disk free (%) and CPU usage (%).
  [85.5][12.0]
 </body>
</html>
```

You would configure the HTTP Content sensor using the mentioned script **URL**, value type **Float**, and number of channels **2**. The sensor will call the URL with every scanning interval and only regard the two values in square brackets *[ ]*, handling each of them in one sensor channel. The additional description text and HTML tags are not necessary; in this example they are added in case a human calls the URL.

Note: If you define the number of channels as **1**, only the first value will be read by the sensor; the second value will be ignored. Using **3** as number of channels will result in a sensor error message.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

HTTP Proxy Settings	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Please enter a string or leave the field empty.
Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either *http:///* or *https:///* or even a simple slash */* as equivalent for *http:///*). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** *www.example.com* and you put a HTTP sensor on it with the value *https:///* in the URL field, PRTG will automatically create the URL *https://www.example.com/* from that. Similarly, if you create a HTTP sensor on the same device using the value */help* in the URL field, PRTG will automatically create and monitor the URL *http://www.example.com/help*

Note: Smart URL replacement does not work for sensors running on the "Probe Device".)

© 2011 Paessler AG

More

Knowledge Base article: How can I monitor internal values of a web application with PRTG?

- http://www.paessler.com/knowledgebase/en/topic/4

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.21 HTTP Full Web Page Sensor

The HTTP Full Web Page sensor monitors the full download time of a web page including images etc. In the background, it opens the web page in Internet Explorer to perform the measurement. Links are not followed. The sensor shows the loading time.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

HTTP Full Web Page Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Full Page Download Settings	
Timeout (sec.)	Enter a timeout in seconds for the HTTP request. If the reply takes longer than this value the request is aborted and an error message is triggered.
URL	Please enter the URL the sensor will load. This address can be independent from the **IP address/DNS name** setting of the device this sensor is created on. PRTG uses a smart URL replacements which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.

© 2011 Paessler AG

Note: The specified web page is loaded in the background in an instance of Internet Explorer. Therefore, the same Internet Explorer settings are used that are configured for the Windows user account the PRTG probe is running on (this is usually the Windows local system user account, if not changed). If you want to e.g. use a proxy for this full web page sensor test, please adjust the Internet Explorer's settings accordingly.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either *http:///* or *https:///* or even a simple slash */* as equivalent for *http:///*). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** *www.example.com* and you put a HTTP sensor on it with the value *https:///* in the URL field, PRTG will automatically create the URL *https://www.example.com/* from that. Similarly, if you create a HTTP sensor on the same device using the value */help* in the URL field, PRTG will automatically create and monitor the URL *http://www.example.com/help*

Note: Smart URL replacement does not work for sensors running on the "Probe Device".)

© 2011 Paessler AG

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.22 HTTP SSL Certificate Expiry Sensor

The HTTP SSL Certificate Expiry Sensor checks a specific https-URL and returns the number of days remaining until the site's SSL certificate expires. It shows a **Warning** when only 60 days are left, and an **Error** status when only 30 days are remaining until the certificate expires.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

HTTP SSL Certificate Expiry Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
URL	Enter the URL to check (this sensor does *not* use the **IP Address/DNS value** of the parent device).
Force SSL V3	Define if you only want to allow SSL V3 connections to the URL defined above. Choose between: ▪ **No** ▪ **Yes**
Timeout (sec.)	Define a timeout in seconds for the entire process. If the reply takes longer than this value the request is aborted and an error message is triggered. Please enter an integer value.

© 2011 Paessler AG

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.23 HTTP Transaction Sensor

The HTTP Transaction sensor monitors an interactive website, such as an web shop, by performing a transaction using a set of Hypertext Transfer Protocol (HTTP) URLs. The sensor monitors whether logins or shopping carts work properly. It returns the loading time.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

HTTP Transaction Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

HTTP Specific	
Timeout (sec.)	Enter a timeout in seconds for all HTTP requests. If the complete transaction takes longer than this value the request is aborted and an error message is triggered.
Single URL Timeout (seconds)	Enter a timeout in seconds for one single HTTP request. If the reply of any single request takes longer than this value the transaction is aborted and an error message is triggered.
SSL Method	This setting is relevant only when using https in the **URL** fields of the transaction URLs below. We recommend using the default value. If you experience connection problems, please select another SSL method from the drop down menu.

Advanced Sensor Data	
Limit Download (kb)	Enter a maximum amount of data that will be transferred per every single request. If you set content checks below, please be aware that only the content downloaded within this limit can be checked for certain search expressions.
Cookie Management	Select if cookies will be used for the transaction. Choose between: • **Use cookies (recommended)**: Allow cookies to be set and read during the transaction cycle. • **Ignore cookies**: Do not allow cookies. Use this option if you want to test the transaction without the use of cookies. We recommend using the default value.

Authentication	
User	If the URL is protected and needs authentication, enter a username here. Please enter a string or leave the field empty.
Password	If the URL is protected and needs authentication, enter a password here. Please enter a string or leave the field empty.
Authentication Method	If you have entered credentials above, please select the authentication method the given URL is protected with. Choose between: • **Basic access authentication (HTTP)**: Use simple HTTP authentication. This is suitable for most cases. • **Windows NT LAN Manager (NTLM)**: Use the Microsoft NTLM protocol for authentication. This is sometimes used in Intranets for single sign-on. We recommend using the default value.

Transaction URL	
You can define up to 10 different transaction URLs which will all be called in a row. Only if the complete transaction can be completed, the sensor will be in an **Up** status. Using this mechanism you can set up an extended monitoring with multiple URLs. Please enter settings for at least one transaction URL. You can use as many URLs as needed and simply leave the other fields empty.	
URL	Please enter the URL the sensor will connect to. This address can be independent from the **IP address/DNS name** setting of the device this sensor is created on. PRTG uses a smart URL replacements which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.
Request Method	The request method determines how the given URL is requested. • **GET**: Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page. • **POST**: Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Postdata** field below.

© 2011 Paessler AG

Transaction URL	
	• **HEAD**: Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.
Response must include	Define which string must be part of the web at the given URL. If the data does not include this string, the sensor will be set to an error state. Please enter a string or leave the field empty.
Response must not include	Define which string must not be part of the web at the given URL. If the data does include this string, the sensor will be set to an error state. Please enter a string or leave the field empty.

HTTP Proxy Settings	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Please enter a string or leave the field empty.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either *http:///* or *https:///* or even a simple slash */* as equivalent for *http:///*). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** *www.example.com* and you put a HTTP sensor on it with the value *https:///* in the URL field, PRTG will automatically create the URL *https://www.example.com/* from that. Similarly, if you create a HTTP sensor on the same device using the value */help* in the URL field, PRTG will automatically create and monitor the URL *http://www.example.com/help*

Note: Smart URL replacement does not work for sensors running on the "Probe Device".)

More

Knowledge Base article: Configuration Tips for HTTP Transaction Sensors needed
- http://www.paessler.com/knowledgebase/en/topic/443

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.24 HTTP XML/REST Value Sensor

The HTTP XML/REST Value sensor retrieves an XML file from a given URL and parses it. It can return the values of specific nodes.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

HTTP XML/REST Value Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
URL	Enter the URL that returns the XML file (this sensor does *not* use the **IP Address/DNS value** of the parent device).
XML Node (and optional property)	Enter the name of the node this sensor will check, or enter a node name and a property name to check a property value.
Max. Response Time	Define a timeout in seconds for the check. If the reply takes longer than this value the request is aborted and an error message is triggered. Please enter an integer value.
HTTP Username	If the URL requires authentication, enter the username. Please enter a string or leave the field empty.

Sensor Settings	
HTTP Password	If the URL requires authentication, enter the password. Please enter a string or leave the field empty.
Sensor Value	Choose between: ▪ **Use the value of the selected XML node**: Return the value found at the specified XML node. If this is non-numeric, you will only see *0*. ▪ **Use the number of occurrences of the selected XML node or its children/siblings**: Return the number of occurrences found.
Characters to Remove	Optionally enter a string which will be removed from the returned XML value. Use this to remove any unwanted characters from the result. Please enter a string or leave the field empty.
Custom Message	Optionally enter a custom sensor message. Use *%1* as a placeholder to automatically fill in the returned XML value. Please enter a string or leave the field empty.
Force SSL V3	Define if you only want to allow SSL V3 connections to the URL defined above. Choose between: ▪ **No** ▪ **Yes**
Timeout (sec.)	Define a timeout in seconds for the entire process. If the reply takes longer than this value the request is aborted and an error message is triggered. Please enter an integer value.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change. • **Trigger 'change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.
Results	Define what will be done with the results given back. Choose between: • **Discard result**: Do not store the requested web page. • **Write result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from to the "Logs (System)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **More** 256 section below.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.25 Hyper-V Host Server Sensor

The Hyper-V Host Server sensor monitors a Microsoft Hyper-V host server. It shows CPU usage in percent of guests, hypervisor, and total, as well as host health critical values, deposited pages, and network traffic. *Note:* The parent device for this sensor must be a Windows Server running Hyper-V.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Hyper-V Host Server Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.26 Hyper-V Virtual Machine Sensor

The Hyper-V Virtual Machine sensor monitors a virtual machine running on a Microsoft Hyper-V host server. It shows CPU usage in percent of guests, hypervisor, and total, as well as disk read and write values, per second. *Note:* The parent device for this sensor must be a Hyper-V server.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Virtual Machine Settings	
Virtual Machine	You see a list of all virtual machines (VMs) available on the host server on this device, including the ones that are not running. All VMs are listed with name and a description. Please choose one or more services by adding a check mark in front of the respective line. For each VM one sensor will be created. *Note:* Please make sure the name of your VMs do not contain unsupported characters, especially avoid the hash ('#') sign. We recommend to not rename virtual machines once you've set up monitoring. For detailed information, please see **More** 336 section below.

Hyper-V Virtual Machine Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Virtual Machine Settings	
GUID	Shows the Globally Unique Identifier (GUID) of the virtual machine monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the virtual machine monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the host server. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Powered Off VMs	Choose how the sensor will react to a virtual machine that is powered off. Please choose between: • **Alarm when powered off (default)**: The sensor will change to a down status if the virtual machine is powered off. • **Ignore powered off state**: The sensor will not change to a down status if the virtual machine is powered off; it will report zero values instead.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

More

Why doesn't my Hyper-V Virtual Machine Sensor work after changing names?
- http://www.paessler.com/knowledgebase/en/topic/15533

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.27 Hyper-V Virtual Storage Device Sensor

The Hyper-V Virtual Storage sensor monitors a virtual storage device running on a Microsoft Hyper-V host server. It shows read and write values in second, and the number of errors. *Note:* The parent device for this sensor must be a Hyper-V server.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Hyper-V Virtual Storage Device Settings	
Hyper-V Virtual Storage Device	You see a list of all virtual storage devices available on the host server on this device. Please choose one or more devices by adding a check mark in front of the respective line. For each storage device one sensor will be created.

Hyper-V Virtual Storage Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Hyper-V Virtual Storage Device Settings	
Virtual Storage Device	Shows the unique name of the device monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.28 IMAP Sensor

The IMAP sensor monitors a mail server using Internet Message Access Protocol (IMAP) and shows the server's response time.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

IMAP Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

IMAP Specific	
Timeout (sec.)	Enter a timeout in seconds for the SMTP connect. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Enter the number of the port that will be used to connect via IMAP. For non-secure connections usually port 143 is used; usually port 993 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.

Authentication	
Authentication Type	Select the kind of authentication for the IMAP connection. Choose between:

Authentication	
	• **Username/Password**: Authenticate at the IMAP server via username and password. • **Simple Authentication and Security Layer (SASL)**: Use a secure connection for the authentication at the IMAP server.
Username	Enter a username for IMAP authentication. Please enter a string.
Password	Enter a password for IMAP authentication. Please enter a string.
TLS (Transport-Level Security)	Choose if a secure connection via TLS/SSL will be used. Choose between • **Don't use** • **Use**
SSL-Method	This field is only visible when TLS is enabled above. Select the SSL method that will be used when connecting to the SMTP server. We recommend using the default value. Only if you experience connection problems, try another setting.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.29 INI File Content Check Sensor

The INI File Content Check sensor reads an *.ini file and returns the value. It indicates if the file exists and if a specified section and field are found. The sensor returns the field's value.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Channel Name	Enter a name for the channel in which the returned values will be shown. This is for display purposes only. Please enter a string.

INI File Content Check Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

Sensor Settings	
INI Filename	Define a path and file name to the INI file. You can either enter an absolute local path or a path in your network. For example, enter *C:\Windows\win.ini*.
INI section	Define the section inside the INI file you would like to check. A section within the INI file is denoted in square brackets *[ ]*. Enter the section name without the brackets here, for example *Mail*.
INI Field	Define the field inside the section you would like to check. In the INI file, a field name is written before an equal sign =, followed by its value. Enter the field name here, for example *MAPI*. The sensor will return the value of this field, i.e. the value on the right side of the equal sign.
Timeout (sec.)	Define a timeout in seconds for the check. If the reply takes longer than this value the request is aborted and an error message is triggered.
Security Context	Define the Windows user account that will be used to run the INI file check. Choose between: • **Use security context of probe service**: Run under the same Windows user account the probe is running on. By default, this is the Windows system user account (if not manually changed). • **Use Windows credentials of parent device**: Use the Windows user account defined in the settings of the parent device this sensor is created on. Please go to sensor's parent device's settings to change these Windows credentials.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change. • **Trigger 'change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.
INI Results	Define what will be done with the result the INI file gives back. Choose between: • **Discard result**: Do not store the requested web page. • **Write result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the script to the "Logs (System)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **More** 256 section below.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor.

Sensor Display	
	▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.30 IP on DNS Blacklist Sensor

The IP on DNS Blacklist sensor checks if the IP address of its parent device is listed on specific blacklist servers and returns the number of hits found. If a DNS name is used as the parent device's hostname, PRTG will resolve it to an IP address first.

During normal operation, there should be *0* hits and the sensor should show a green **OK** status. If the IP address is found by at least one of the blacklist servers, the sensor changes to a red **Down** status.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

INI File Content Check Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Blacklist Servers	Define the blacklist servers that will be used for the check. You can enter a comma separated list. If left empty, PRTG will automatically use all of the following servers: *sbl-xbl.spamhaus.org, bl.spamcop.net, dnsbl.njabl.org, list.dsbl.org, multihop.dsbl.org, list.dsbl.org and multihop.dsbl.org*
Timeout (sec.)	Define a timeout in seconds for the check. If the reply takes longer than this value the request is aborted and an error message is triggered.

© 2011 Paessler AG

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.31 jFlow V5 Sensor

The jFlow V5 sensor receives traffic data from a jFlow V5 compatible device and shows the traffic by type. On your hardware device, please make sure it matches jFlow V5 and disable any sampling option! There are several filter options available to divide traffic into different channels.

Note: In order for the sensor to work, jFlow export of the respective version must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe). The sensor does not support sampling, so please disable sampling in your jFlow device!

For a general introduction to the technology behind flow monitoring, please see **Monitoring Bandwidth via Flows** 942 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

jFlow V5 Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

jFlow V5 Specific Settings	
Receive jFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the jFlow export options of your hardware router device. Please enter an integer value. Please use a different port for each jFlow device, as traffic is distinguished by port, not by IP address! *Note:* When configuring export, please make sure you select the appropriate jFlow version for this sensor.

jFlow V5 Specific Settings	
Receive jFlow Packets on IP	Select the IP address(es) on which PRTG listens to jFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the jFlow export options of your hardware router device. *Note:* When configuring export, please make sure you select the appropriate jFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an **Unknown** status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. *Note:* If you set this value too low, flow information might get lost!
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to disk. Choose between: ▪ **None (recommended)**: Do not write additional log files. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write log files of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write log files for all data received. *Note:* Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.
Channel Configuration	
Channel Selection	Define the categories the traffic will be accounted to. There are different groups of traffic available. Choose between: ▪ **Web**: Internet web traffic. ▪ **File Transfer**: Traffic caused by FTP. ▪ **Mail**: Internet mail traffic. ▪ **Chat**: Traffic caused by chat and instant messaging. ▪ **Remote Control**: Traffic caused by remote control applications, such as RDP, SSH, Telnet, VNC. ▪ **Infrastructure**: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, SNMP. ▪ **NetBIOS**: Traffic caused by NetBIOS communication. ▪ **Other Protocols**: Traffic caused by various other protocols via UDP and TCP. For each traffic group, you can select how many channels will be used for each group, i.e. how detailed traffic will be divided. For each group, choose between: ▪ **No**: Do not account traffic of this group in an own channel. All traffic of this group will be accounted to the default channel named **Other**. ▪ **Yes**: Count all traffic of this group and summarize it into one channel. ▪ **Detail**: Count all traffic of this group and further divide it into different channels. The traffic will appear in several channels as shown in the **Content** column. *Note:* Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyse.

© 2011 Paessler AG

Filtering	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps and initially when selecting the **Toplists** tab. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ *[Any custom toplists you have added]*

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Toplists

For all xFlow and packet sniffer sensors, there is a **Toplists** tab available. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see Toplists 807 section.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

Related Topics

- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Channel Defintions for xFlow and Packet Sniffer Sensors 982

© 2011 Paessler AG

6.7.32 jFlow V5 (Custom) Sensor

The jFlow V5 (Custom) sensor receives traffic data from a jFlow V5 compatible device and shows the traffic by type. On your hardware device, please make sure it matches jFlow V5 and disable any sampling option! In this custom sensor, you can define your own channel definitions to divide traffic into different channels.

Note: In order for the sensor to work, jFlow export of the respective version must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe). The sensor does not support sampling, so please disable sampling in your jFlow device!

For a general introduction to the technology behind flow monitoring, please see **Monitoring Bandwidth via Flows** 942 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

jFlow V5 (Custom) Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

jFlow Specific Settings	
Receive jFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one configured in the jFlow export options of your hardware router device. Please enter an integer value. Please use a different port for each jFlow device, as traffic is distinguished by port, not by IP address! *Note:* When configuring export, please make sure you select the appropriate jFlow version for this sensor.
Receive jFlow Packets on IP	Select the IP address(es) on which PRTG listens to jFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the jFlow export options of your hardware router device. *Note:* When configuring export, please make sure you select the appropriate jFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an **Unknown** status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. *Note:* If you set this value too low, flow information might get lost!
Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see Channel Defintions for xFlow and Packet Sniffer Sensors 982 section. All traffic for which no channel is defined will be accounted to the default channel named **Other**. *Note:* Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyse.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to disk. Choose between: ▪ **None (recommended)**: Do not write additional log files. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write log files of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write log files for all data received. *Note:* Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Filtering	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.

© 2011 Paessler AG

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps and initially when selecting the **Toplists** tab. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ ***[Any custom toplists you have added]***

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Toplists

For all xFlow and packet sniffer sensors, there is a **Toplists** tab available. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see section

- Toplists 807

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

Related Topics

- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Channel Defintions for xFlow and Packet Sniffer Sensors 982

© 2011 Paessler AG

6.7.33 LDAP Sensor

The LDAP sensor monitors directory services using Lightweight Directory Access Protocol (LDAP), connecting to the server trying a "bind". It shows the response time. If the server does not respond or authentication fails, an error message will be triggered.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

LDAP Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

LDAP Specific	
Port	Enter the LDAP port number, usually port 389 for unencrypted connections. Please enter an integer value.
Distinguished Name	Enter the distinguished name (DN) you want to authenticate to the LDAP server. Usually, this is the information for the user you want to authenticate with. For example, use the format **cn=Manager,dc=my-domain,dc=com** for a DN on an OpenLDAP server.
Passwort	Enter the password for the entered Distinguished Name.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.34 Logfile Content Check Sensor

The Logfile Content Check sensor checks a text file for certain strings and returns either a status code or the line number of a match. Additionally, matching lines can be quoted to the sensor message field.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Channel Name	Enter a name for the channel in which the returned values will be shown. This is for display purposes only. Please enter a string.

Logfile Content Check Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

Sensor Settings	
Log Filename	Define a path and file name to the log file. You can either enter an absolute local path or a path in your network. For example, enter *C:\Windows\security\logs*.
Search String	Define the string inside the log file you would like to check for. The input is *not* case-sensitive. Please enter a string.
Search Method	Define the method you want to provide the search string with. The pattern must be contained in *one* line and only the *last* matching line will be given back. Choose between: ▪ **Simple String Search**: Search for a simple string. ▪ **Regular Expression**: Search using a regular expression. For more details, see Regular Expressions 985 section.
Sensor Value	Define which kind of numbers will be given back in the sensor channel. Choose between: ▪ **Return a status code**: Returns *0* for no match, *1* for a match that was found before, and *2* for at least one new match found (since last check). ▪ **Return line containing the string**: Returns the line number of a match. If several matches are found, only the line number of the last match is shown. If no match is found, the value is *0*.
Sensor Message	Define which kind of text will shown in the sensor message. Choose between: ▪ **Status**: Show a status text, for example, *New match found at line x*. ▪ **Line from file that contained the search string**: Returns the line containing a match. If several matches are found, only the line of the last match is shown. If there is no match, the sensor message will be *No match found*.
Timeout (sec.)	Define a timeout in seconds for the check. If the reply takes longer than this value the request is aborted and an error message is triggered. Please enter an integer value.
Security Context	Define the Windows user account that will be used to run the INI file check. Choose between: • **Use security context of probe service**: Run under the same Windows user account the probe is running on. By default, this is the Windows system user account (if not manually changed). • **Use Windows credentials of parent device**: Use the Windows user account defined in the settings of the parent device this sensor is created on. Please go to sensor's parent device's settings to change these Windows credentials.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change.

Sensor Settings	
	• **Trigger 'change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.
Log Results	Define what will be done with the result the log file gives back. Choose between: • **Discard result**: Do not store the requested web page. • **Write result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the script to the "Logs (System)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **More** 256 section below.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.35 Microsoft SQL Sensor

The Microsoft SQL sensor monitors a Microsoft Structured Query Language (SQL) server. It shows the response time, the number of records, and the value. The sensor can monitor if the database server accepts connections, processes requests, and returns an expected result when executing a custom SQL command.

The following SQL servers are supported: SQL Server 2008, SQL Server 2005 (including SQL Server Express / Server Compact Editions), SQL Server 2000, SQL Server 7 and MSDE (requires OLE DB installed on the machine running the PRTG probe that accesses the server)

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Microsoft SQL Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SQL-Server Specific Data	
Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

© 2011 Paessler AG

SQL-Server Specific Data	
Instance	Enter the SQL server instance's name if you want to connect to a "named instance". For example, such an instance's name could be *SQLEXPRESS*. *Note:* Sometimes you will see connection strings like *SQLSERVER\SQLINSTANCE* in database clients. The first part is the server name configured under the general server settings. The second part refers to the instance name mentioned above. Never enter this complete string in this PRTG form, merely provide the second part (without the backslash). Please enter a string or leave the field empty.
Port	Define the port for the SQL connection. Choose between: ▪ **Automatic**: Automatically choose the right port. ▪ **Manual**: Use a specific port. Define below. Standard value is **1433**.
Port	This field is only visible if manual port selection is enabled above. Define the port number for the SQL connection. Please enter an integer value.

Database	
Database	Enter the name of the SQL database the sensor will connect to. For example, such a database's name could be *Northwind*
Authentication	Define the kind of authentication used for the connection to the database. Choose between: ▪ **SQL Server**: Use credentials specific to the SQL server. Please enter them below. ▪ **Windows Authentication**: Use the Windows credentials defined for the parent device this sensor is created on. *Note:* For successful authentication, the defined Windows credentials must be known to the SQL server, and SQL server and the computer the PRTG probe is running on must be in the same domain.
User	This field is only visible if SQL server authentication is enabled above. Enter the user name that will be used for the database connection.
Password	This field is only visible if SQL server authentication is enabled above. Enter the password that will be used for the database connection.

Data	
SQL-Expression	Enter the SQL expression that will be queried from the database. For example, such an expression could be: *SELECT ProductName FROM Northwind.dbo.Products*. *Note:* When a cursor is returned (i.e. with a SELECT statement), only the first row of data will be processed.

Postprocessing	If the SQL expression returns a result set, please define if you want to further process it. Choose between: ▪ **Ignore result set**: Do not do anything with the data returned. ▪ **Process numerical result**: Regard the result set returned as integer or float. You can set the sensor to **Warning** or **Down** status for specific thresholds. Define below. ▪ **Process string result**: Regard the result set returned as a string. You can set the sensor to error for certain sub-strings contained or missing. Define below. ▪ **Monitor for changes**: Monitor if the result set has changed since last check. The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever a sensor value changes.
Condition "Warning"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a **Warning** status. Choose between: ▪ **none**: Do not set the sensor to **Warning** status for any condition. ▪ **equals**: Result set must be the same as the value provided below. ▪ **is above**: Result set must be above the value provided below. ▪ **lower than**: Result set must be below the value provided below. ▪ **does not equal**: Result set must be unequal to the value provided below. *Note:* This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings 792.
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor into a **Warning** status. Please enter an integer or float value.
Condition "Down"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a **Down** status. Choose between: ▪ **none**: Do not set the sensor to **Down** status for any condition. ▪ **equals**: Result set must be the same as the value provided below. ▪ **is above**: Result set must be above the value provided below. ▪ **lower than**: Result set must be below the value provided below. ▪ **does not equal**: Result set must be unequal to the value provided below. *Note:* This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings 792.
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor to a **Down** status. Please enter an integer value.
Response must include	This field is only visible if string results is enabled above. Enter a string that must be part of the returned SQL string. If it is not, the sensor will be set to an error state. Please enter a string or leave the field empty.
Response must not include	This field is only visible if string results is enabled above. Enter a string that must not be part of the returned SQL string. If it is, the sensor will be set to an error state. Please enter a string or leave the field empty.

© 2011 Paessler AG

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.36 MySQL Sensor

The MySQL sensor monitors a MySQL server. It connects to the server and shows the response time. Additionally, it can read the number of records and a value.

The following SQL servers are supported: MySQL server 5.1, 5.0, 4.1, 4.0, and 3.23

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

MySQL Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

MySQL Server Specific Data	
Port	Define the port for the SQL connection. Choose between: ▪ **Automatic**: Automatically choose the right port. ▪ **Manual**: Use a specific port. Define below. Standard value is **3306**.
Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

DB/SQL Data	
Database	Enter the name of the SQL database the sensor will connect to. For example, such a database's name could be *MyDatabase*. This is a logical entity on the database server where database objects like tables or stored procedures exist. In case of the mySQL server it also reflects a physical directory structure where your database objects are stored. Enter the appropriate string which is the same as you would supply when invoking the *mysql.exe* admin tool (with the command line switch *-p*) or after the login with *mysql.exe* with the command *use*.
User	Enter the user name that will be used for the database connection.
Password	Enter the password that will be used for the database connection.

Data	
SQL-Expression	Enter the SQL expression that will be queried from the database. For example, such an expression could be: *SELECT AVG(UnitPrice) FROM Products*. *Note:* When a cursor is returned (i.e. with a SELECT statement), only the first row of data will be processed.
Postprocessing	If the SQL expression returns a result set, please define if you want to further process it. Choose between: ▪ **Ignore result set**: Do not do anything with the data returned. ▪ **Process numerical result**: Regard the result set returned as integer or float. You can set the sensor to **Warning** or **Down** status for specific thresholds. Define below. ▪ **Process string result**: Regard the result set returned as a string. You can set the sensor to error for certain sub-strings contained or missing. Define below. ▪ **Monitor for changes**: Monitor if the result set has changed since last check. The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever a sensor value changes.
Condition "Warning"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a **Warning** status. Choose between: ▪ **none**: Do not set the sensor to **Warning** status for any condition. ▪ **equals**: Result set must be the same as the value provided below. ▪ **is above**: Result set must be above the value provided below. ▪ **lower than**: Result set must be below the value provided below. ▪ **does not equal**: Result set must be unequal to the value provided below. *Note:* This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings 792.
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor into a **Warning** status. Please enter an integer or float value.

© 2011 Paessler AG

Postprocessing	If the SQL expression returns a result set, please define if you want to further process it. Choose between: ▪ **Ignore result set**: Do not do anything with the data returned. ▪ **Process numerical result**: Regard the result set returned as integer or float. You can set the sensor to **Warning** or **Down** status for specific thresholds. Define below. ▪ **Process string result**: Regard the result set returned as a string. You can set the sensor to error for certain sub-strings contained or missing. Define below. ▪ **Monitor for changes**: Monitor if the result set has changed since last check. The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever a sensor value changes.
Condition "Down"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a **Down** status. Choose between: ▪ **none**: Do not set the sensor to **Down** status for any condition. ▪ **equals**: Result set must be the same as the value provided below. ▪ **is above**: Result set must be above the value provided below. ▪ **lower than**: Result set must be below the value provided below. ▪ **does not equal**: Result set must be unequal to the value provided below. *Note:* This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings 792.
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor to a **Down** status. Please enter an integer value.
Response must include	This field is only visible if string results is enabled above. Enter a string that must be part of the returned SQL string. If it is not, the sensor will be set to an error state. Please enter a string or leave the field empty.
Response must not include	This field is only visible if string results is enabled above. Enter a string that must not be part of the returned SQL string. If it is, the sensor will be set to an error state. Please enter a string or leave the field empty.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Note: For this sensor type, no port number can be set.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.37 NetFlow V5 Sensor

The NetFlow V5 sensor receives traffic data from a NetFlow V5 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! There are several filter options available to divide traffic into different channels.

Note: In order for the sensor to work, NetFlow export of the respective version must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).

For a general introduction to the technology behind flow monitoring, please see **Monitoring Bandwidth via Flows** 942 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

NetFlow V5 Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetFlow Specific Settings	
Receive NetFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the NetFlow export options of your hardware router device. Please enter an integer value. Please use a different port for each NetFlow device, as traffic is distinguished by port, not by IP address! *Note:* When configuring export, please make sure you select the appropriate NetFlow version for this sensor.

© 2011 Paessler AG

NetFlow Specific Settings	
Receive NetFlow Packets on IP	Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the NetFlow export options of your hardware router device. *Note:* When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an **Unknown** status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. *Note:* If you set this value too low, flow information might get lost!
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to disk. Choose between: ▪ **None (recommended)**: Do not write additional log files. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write log files of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write log files for all data received. *Note:* Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.
Channel Configuration	
Channel Selection	Define the categories the traffic will be accounted to. There are different groups of traffic available. Choose between: ▪ **Web**: Internet web traffic. ▪ **File Transfer**: Traffic caused by FTP. ▪ **Mail**: Internet mail traffic. ▪ **Chat**: Traffic caused by chat and instant messaging. ▪ **Remote Control**: Traffic caused by remote control applications, such as RDP, SSH, Telnet, VNC. ▪ **Infrastructure**: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, SNMP. ▪ **NetBIOS**: Traffic caused by NetBIOS communication. ▪ **Other Protocols**: Traffic caused by various other protocols via UDP and TCP. For each traffic group, you can select how many channels will be used for each group, i.e. how detailed traffic will be divided. For each group, choose between: ▪ **No**: Do not account traffic of this group in an own channel. All traffic of this group will be accounted to the default channel named **Other**. ▪ **Yes**: Count all traffic of this group and summarize it into one channel. ▪ **Detail**: Count all traffic of this group and further divide it into different channels. The traffic will appear in several channels as shown in the **Content** column. *Note:* Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyse.

Filtering	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps and initially when selecting the **Toplists** tab. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ *[Any custom toplists you have added]*

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Toplists

For all xFlow and packet sniffer sensors, there is a **Toplists** tab available. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see Toplists 807 section.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

© 2011 Paessler AG

Others

For more general information about settings, please see Object Settings 111 section.

Related Topics

- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Channel Defintions for xFlow and Packet Sniffer Sensors 982

6.7.38 NetFlow V5 (Custom) Sensor

The NetFlow V5 (Custom) sensor receives traffic data from a NetFlow V5 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! In this custom sensor, you can define your own channel definitions to divide traffic into different channels.

Note: In order for the sensor to work, NetFlow export of the respective version must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).

For a general introduction to the technology behind flow monitoring, please see **Monitoring Bandwidth via Flows** 942 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

NetFlow V5 (Custom) Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetFlow Specific Settings	
Receive NetFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one configured in the NetFlow export options of your hardware router device. Please enter an integer value. Please use a different port for each NetFlow device, as traffic is distinguished by port, not by IP address! *Note:* When configuring export, please make sure you select the appropriate NetFlow version for this sensor.

© 2011 Paessler AG

NetFlow Specific Settings	
Receive NetFlow Packets on IP	Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the NetFlow export options of your hardware router device. *Note:* When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an **Unknown** status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. *Note:* If you set this value too low, flow information might get lost!
Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see Channel Defintions for xFlow and Packet Sniffer Sensors 982 section. All traffic for which no channel is defined will be accounted to the default channel named **Other**. *Note:* Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyse.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to disk. Choose between: ▪ **None (recommended)**: Do not write additional log files. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write log files of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write log files for all data received. *Note:* Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Filtering	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps and initially when selecting the **Toplists** tab. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ ***[Any custom toplists you have added]***

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Toplists

For all xFlow and packet sniffer sensors, there is a **Toplists** tab available. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see section

- Toplists 807

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

© 2011 Paessler AG

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

Related Topics

- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Channel Defintions for xFlow and Packet Sniffer Sensors 982

6.7.39 NetFlow V9 Sensor

The NetFlow V9 sensor receives traffic data from a NetFlow V9 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! There are several filter options available to divide traffic into different channels.

Note: In order for the sensor to work, NetFlow export of the respective version must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).

For a general introduction to the technology behind flow monitoring, please see **Monitoring Bandwidth via Flows** 942 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

NetFlow V9 Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetFlow Specific Settings	
Receive NetFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the NetFlow export options of your hardware router device. Please enter an integer value. Please use a different port for each NetFlow device, as traffic is distinguished by port, not by IP address! *Note:* When configuring export, please make sure you select the appropriate NetFlow version for this sensor.

© 2011 Paessler AG

NetFlow Specific Settings	
Receive NetFlow Packets on IP	Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the NetFlow export options of your hardware router device. *Note:* When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an **Unknown** status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. *Note:* If you set this value too low, flow information might get lost!
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to disk. Choose between: ▪ **None (recommended)**: Do not write additional log files. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write log files of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write log files for all data received. *Note:* Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.
Channel Configuration	
Channel Selection	Define the categories the traffic will be accounted to. There are different groups of traffic available. Choose between: ▪ **Web**: Internet web traffic. ▪ **File Transfer**: Traffic caused by FTP. ▪ **Mail**: Internet mail traffic. ▪ **Chat**: Traffic caused by chat and instant messaging. ▪ **Remote Control**: Traffic caused by remote control applications, such as RDP, SSH, Telnet, VNC. ▪ **Infrastructure**: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, SNMP. ▪ **NetBIOS**: Traffic caused by NetBIOS communication. ▪ **Other Protocols**: Traffic caused by various other protocols via UDP and TCP. For each traffic group, you can select how many channels will be used for each group, i.e. how detailed traffic will be divided. For each group, choose between: ▪ **No**: Do not account traffic of this group in an own channel. All traffic of this group will be accounted to the default channel named **Other**. ▪ **Yes**: Count all traffic of this group and summarize it into one channel. ▪ **Detail**: Count all traffic of this group and further divide it into different channels. The traffic will appear in several channels as shown in the **Content** column. *Note:* Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyse.

Filtering	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps and initially when selecting the **Toplists** tab. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ *[Any custom toplists you have added]*

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Toplists

For all xFlow and packet sniffer sensors, there is a **Toplists** tab available. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see Toplists 807 section.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

© 2011 Paessler AG

Others

For more general information about settings, please see Object Settings 111 section.

Related Topics

- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Channel Defintions for xFlow and Packet Sniffer Sensors 982

6.7.40 NetFlow V9 (Custom) Sensor

The NetFlow V9 (Custom) sensor receives traffic data from a NetFlow V9 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! In this custom sensor, you can define your own channel definitions to divide traffic into different channels.

Note: In order for the sensor to work, NetFlow export of the respective version must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).

For a general introduction to the technology behind flow monitoring, please see **Monitoring Bandwidth via Flows** 942 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

NetFlow V9 (Custom) Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetFlow Specific Settings	
Receive NetFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one configured in the NetFlow export options of your hardware router device. Please enter an integer value. Please use a different port for each NetFlow device, as traffic is distinguished by port, not by IP address! *Note:* When configuring export, please make sure you select the appropriate NetFlow version for this sensor.

© 2011 Paessler AG

NetFlow Specific Settings	
Receive NetFlow Packets on IP	Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the NetFlow export options of your hardware router device. *Note:* When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an **Unknown** status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. *Note:* If you set this value too low, flow information might get lost!
Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see Channel Defintions for xFlow and Packet Sniffer Sensors 982 section. All traffic for which no channel is defined will be accounted to the default channel named **Other**. *Note:* Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyse.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to disk. Choose between: ▪ **None (recommended)**: Do not write additional log files. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write log files of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write log files for all data received. *Note:* Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Filtering	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps and initially when selecting the **Toplists** tab. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ ***[Any custom toplists you have added]***

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Toplists

For all xFlow and packet sniffer sensors, there is a **Toplists** tab available. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see section

- Toplists 807

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

© 2011 Paessler AG

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

Related Topics

- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Channel Defintions for xFlow and Packet Sniffer Sensors 982

6.7.41 NTP Sensor

The NTP Sensor monitors a Network Time Protocol (NTP) server. It returns the response time and the time difference in comparison to the local system time.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

NTP Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NTP Specific	
Timeout (sec.)	Enter a timeout in seconds. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Enter the NTP port. Usually port 1024 is used. We recommend using the default value.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.42 Oracle SQL Sensor

The Oracle SQL sensor monitors an Oracle SQL server. It connects to the server and shows the response time. Additionally, it can read the number of records and a value.

The following SQL servers are supported: Supports Oracle servers 11g, 10g, 9i, 8i, 8.0, and 7.3, including Oracle 10g Express, and Oracle 8i Personal and Lite editions (requires default TCP port setting *1521*).

Note: On the client computer running the PRTG probe where this sensor is created on, *Oracle Net* is used for direct TCP/IP communication; OCI is not supported any more. You do not need to install an Oracle client or define a *TNSNAMES.ORA* on the client computer.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Oracle Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Oracle Specific Data	
Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Enter the port number that will be used for the connection. Default value is **1521**. Please enter an integer value.

DB/SQL Data	
Database	Enter the name of the SQL database the sensor will connect to. For example, such a database's name could be *orcl*
User	Enter the user name that will be used for the database connection.
Password	Enter the password that will be used for the database connection.

Data	
SQL-Expression	Enter the SQL expression that will be queried from the database. For example, such an expression could be: *SELECT sum(salary) FROM hr.employees*. *Note:* When a cursor is returned (i.e. with a SELECT statement), only the first row of data will be processed.
Postprocessing	If the SQL expression returns a result set, please define if you want to further process it. Choose between: ▪ **Ignore result set**: Do not do anything with the data returned. ▪ **Process numerical result**: Regard the result set returned as integer or float. You can set the sensor to **Warning** or **Down** status for specific thresholds. Define below. ▪ **Process string result**: Regard the result set returned as a string. You can set the sensor to error for certain sub-strings contained or missing. Define below. ▪ **Monitor for changes**: Monitor if the result set has changed since last check. The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever a sensor value changes.
Condition "Warning"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a **Warning** status. Choose between: ▪ **none**: Do not set the sensor to **Warning** status for any condition. ▪ **equals**: Result set must be the same as the value provided below. ▪ **is above**: Result set must be above the value provided below. ▪ **lower than**: Result set must be below the value provided below. ▪ **does not equal**: Result set must be unequal to the value provided below. *Note:* This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings 792.
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor into a **Warning** status. Please enter an integer or float value.
Condition "Down"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a **Down** status. Choose between: ▪ **none**: Do not set the sensor to **Down** status for any condition. ▪ **equals**: Result set must be the same as the value provided below. ▪ **is above**: Result set must be above the value provided below. ▪ **lower than**: Result set must be below the value provided below.

© 2011 Paessler AG

Postprocessing	If the SQL expression returns a result set, please define if you want to further process it. Choose between: ▪ **Ignore result set**: Do not do anything with the data returned. ▪ **Process numerical result**: Regard the result set returned as integer or float. You can set the sensor to **Warning** or **Down** status for specific thresholds. Define below. ▪ **Process string result**: Regard the result set returned as a string. You can set the sensor to error for certain sub-strings contained or missing. Define below. ▪ **Monitor for changes**: Monitor if the result set has changed since last check. The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever a sensor value changes.
	▪ **does not equal**: Result set must be unequal to the value provided below. *Note:* This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings 792.
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor to a **Down** status. Please enter an integer value.
Response must include	This field is only visible if string results is enabled above. Enter a string that must be part of the returned SQL string. If it is not, the sensor will be set to an error state. Please enter a string or leave the field empty.
Response must not include	This field is only visible if string results is enabled above. Enter a string that must not be part of the returned SQL string. If it is, the sensor will be set to an error state. Please enter a string or leave the field empty.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.43 Pingdom Sensor

The Pingdom sensor queries an account at Pingdom.com and retrieves values for one "check" configured in the respective Pingdom account. With every scanning interval, the sensor will always catch the last value available in the "detailed check log" of your Pingdom account.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Pingdom Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Pingdom Check Name	Enter the name of the "check" you want to retrieve data for. Enter it exactly the way configured in your Pingdom account. This setting is case sensitive! Please enter a string.
Username	Please enter the username of the Pingdom account you want to query. Please enter a string.
Password	Please enter the password of the Pingdom account you want to query. Please enter a string.

Sensor Settings	
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change. • **Trigger 'change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871. *Note:* Please make sure you select the same scanning interval you configured for the "check" in your Pingdom account. Only if the intervals match PRTG can catch every measurement from your "check".

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.44 Packet Sniffer (Content) Sensor

Monitors the content of data packets passing a local network card using built-in packet sniffer. You can choose from predefined channels. The full content of packets will be analyzed. If you are searching for a sensor that causes less load on the probe system please consider using the **Packet Sniffer (Header) Sensor** 446.

Note: This sensor can be set up on a Probe Device only! By default, you can only monitor traffic passing the PRTG probe system on which's **Probe Device** the sensor is set up (either a local or remote probe). To monitor other traffic in your network, you can configure a monitoring port (if available) to which the switch sends a copy of all traffic. You can then physically connect this port to a network card of the computer the PRTG probe (either local or remote probe) is running on. This way, PRTG will be able to analyze the complete traffic that passes through the switch. This feature of your hardware may be called Switched Port Analyzer (SPAN), port mirroring, or port monitoring.

For a general introduction to the technology behind packet sniffing, please see **Monitoring Bandwidth via Packet Sniffing** 940 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Packet Sniffer (Content) Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

Sniffer specific	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Network Adapters	Define the network adapters that will be monitored by the sensor. You see a list of names with all adapters available on the probe system. To select an adapter, set a check mark symbol in front of the respective name.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to disk. Choose between: ▪ **None (recommended)**: Do not write additional log files. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write log files of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write log files for all data received. *Note:* Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Channel Configuration	
Channel Selection	Define the categories the traffic will be accounted to. There are different groups of traffic available. Choose between: ▪ **Web**: Internet web traffic. ▪ **File Transfer**: Traffic caused by FTP. ▪ **Mail**: Internet mail traffic. ▪ **Chat**: Traffic caused by chat and instant messaging. ▪ **Remote Control**: Traffic caused by remote control applications, such as RDP, SSH, Telnet, VNC. ▪ **Infrastructure**: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, SNMP. ▪ **NetBIOS**: Traffic caused by NetBIOS communication. ▪ **Other Protocols**: Traffic caused by various other protocols via UDP and TCP. For each traffic group, you can select how many channels will be used for each group, i.e. how detailed traffic will be divided. For each group, choose between: ▪ **No**: Do not account traffic of this group in an own channel. All traffic of this group will be accounted to the default channel named **Other**. ▪ **Yes**: Count all traffic of this group and summarize it into one channel. ▪ **Detail**: Count all traffic of this group and further divide it into different channels. The traffic will appear in several channels as shown in the **Content** column. *Note:* Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyse.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps and initially when selecting the **Toplists** tab. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ *[Any custom toplists you have added]*

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Toplists

For all xFlow and packet sniffer sensors, there is a **Toplists** tab available. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see Toplists 807 section.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

© 2011 Paessler AG

Others

For more general information about settings, please see Object Settings 111 section.

Related Topics

- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Channel Defintions for xFlow and Packet Sniffer Sensors 982

6.7.45 Packet Sniffer (Custom) Sensor

Monitors the custom content of data packets passing a local network card using built-in packet sniffer. You can define your own channels. There are no predefined channels for this sensor type.

Note: This sensor can be set up on a Probe Device only! By default, you can only monitor traffic passing the PRTG probe system on which's **Probe Device** the sensor is set up (either a local or remote probe).To monitor other traffic in your network, you can configure a monitoring port (if available) to which the switch sends a copy of all traffic. You can then physically connect this port to a network card of the computer the PRTG probe (either local or remote probe) is running on. This way, PRTG will be able to analyze the complete traffic that passes through the switch. This feature of your hardware may be called Switched Port Analyzer (SPAN), port mirroring, or port monitoring.

For a general introduction to the technology behind packet sniffing, please see **Monitoring Bandwidth via Packet Sniffing** 940 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Packet Sniffer (Custom) Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sniffer specific	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see **Filter Rules for xFlow and Packet Sniffer Sensors** 980 section.

© 2011 Paessler AG

Sniffer specific	
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see Channel Defintions for xFlow and Packet Sniffer Sensors 982 section. All traffic for which no channel is defined will be accounted to the default channel named **Other**. *Note:* Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyse.
Network Adapters	Define the network adapters that will be monitored by the sensor. You see a list of names with all adapters available on the probe system. To select an adapter, set a check mark symbol in front of the respective name.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to disk. Choose between: ▪ **None (recommended)**: Do not write additional log files. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write log files of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write log files for all data received. *Note:* Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps and initially when selecting the **Toplists** tab. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ *[Any custom toplists you have added]*

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Toplists

For all xFlow and packet sniffer sensors, there is a **Toplists** tab available. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see Toplists 807 section.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

© 2011 Paessler AG

Others

For more general information about settings, please see Object Settings 111 section.

Related Topics

- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Channel Defintions for xFlow and Packet Sniffer Sensors 982

6.7.46 Packet Sniffer (Header) Sensor

Monitors the headers of data packets passing a local network card using built-in packet sniffer. You can choose from predefined channels. Only header traffic will be analyzed, which creates less load on the probe system than the Packet Sniffer (Content) Sensor 434 or Packet Sniffer (Custom) Sensor 440.

Note: This sensor can be set up on a Probe Device only! By default, you can only monitor traffic passing the PRTG probe system on which's **Probe Device** the sensor is set up (either a local or remote probe). To monitor other traffic in your network, you can configure a monitoring port (if available) to which the switch sends a copy of all traffic. You can then physically connect this port to a network card of the computer the PRTG probe (either local or remote probe) is running on. This way, PRTG will be able to analyze the complete traffic that passes through the switch. This feature of your hardware may be called Switched Port Analyzer (SPAN), port mirroring, or port monitoring.

For a general introduction to the technology behind packet sniffing, please see Monitoring Bandwidth via Packet Sniffing 940 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Packet Sniffer (Header) Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

Sniffer specific	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Network Adapters	Define the network adapters that will be monitored by the sensor. You see a list of names with all adapters available on the probe system. To select an adapter, set a check mark symbol in front of the respective name.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to disk. Choose between: ▪ **None (recommended)**: Do not write additional log files. Recommended for normal use cases. ▪ **Only for the 'Other' channel**: Only write log files of data that is not filtered otherwise and therefore accounted to the default **Other** channel. ▪ **All stream data**: Write log files for all data received. *Note:* Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Channel Configuration	
Channel Selection	Define the categories the traffic will be accounted to. There are different groups of traffic available. Choose between: ▪ **Web**: Internet web traffic. ▪ **File Transfer**: Traffic caused by FTP. ▪ **Mail**: Internet mail traffic. ▪ **Chat**: Traffic caused by chat and instant messaging. ▪ **Remote Control**: Traffic caused by remote control applications, such as RDP, SSH, Telnet, VNC. ▪ **Infrastructure**: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, SNMP. ▪ **NetBIOS**: Traffic caused by NetBIOS communication. ▪ **Other Protocols**: Traffic caused by various other protocols via UDP and TCP. For each traffic group, you can select how many channels will be used for each group, i.e. how detailed traffic will be divided. For each group, choose between: ▪ **No**: Do not account traffic of this group in an own channel. All traffic of this group will be accounted to the default channel named **Other**. ▪ **Yes**: Count all traffic of this group and summarize it into one channel. ▪ **Detail**: Count all traffic of this group and further divide it into different channels. The traffic will appear in several channels as shown in the **Content** column. *Note:* Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyse.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps and initially when selecting the **Toplists** tab. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ *[Any custom toplists you have added]*

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Toplists

For all xFlow and packet sniffer sensors, there is a **Toplists** tab available. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see Toplists 807 section.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

© 2011 Paessler AG

Others

For more general information about settings, please see Object Settings 111 section.

Related Topics

- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Channel Defintions for xFlow and Packet Sniffer Sensors 982

6.7.47 Ping Sensor

The Ping sensor performs one or more Pings to monitor the availability of a device. When using more than one Ping per interval, it also measures occurring packet loss in percent.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Ping Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Ping Settings	
Timeout (seconds)	Enter a timeout in seconds for the Ping. If the reply takes longer than this value the request is aborted and an error message is triggered.
Packet Size (Bytes)	Enter the packet size in bytes for the Ping. You can choose any value between 1 and 10000. We recommend using the default value.
Ping Count	Enter the number of Pings that are sent in a row for one interval. "1" is good for availability monitoring. If you want to measure packet loss, enter a higher value. Also enter a higher value than 1 if you want to create reports 88 about average Ping times out of a series of ping requests.
Auto Acknowledge	You can define that a **Down** status of this sensor will be acknowledged 114 automatically. ▪ **Show "Down" status on error (default)**: Do not automatically acknowledge an alarm if this sensor changes to a **Down** status.

© 2011 Paessler AG

Ping Settings	
	▪ **Show "Down (Acknowledged)" status on error**: Automatically acknowledge an alarm. If this sensor changes to a **Down** status, it will automatically change to **Down (Acknowledged)**. *Note:* The sensor will also go through a **Down** status, so any sensor state triggers 797 using this will still provoke notifications, as configured.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

More

Knowledge Base: How to create/customize statistical PING sensor?
- http://www.paessler.com/knowledgebase/en/topic/1873

Knowledge Base: Can I create an inverse Ping sensor?
- http://www.paessler.com/knowledgebase/en/topic/10203

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.48 Ping Jitter Sensor

The Ping Jitter sensor sends a series of Pings to the given URI to determine the statistical jitter. The Real Time Jitter value is updated every time a packet is received using the formula described in RFC 1889:

Jitter = Jitter + (abs(ElapsedTime - OldElapsedTime) - Jitter) / 16

The Statistical Jitter value is calculated on the first xx packets received using the statistical variance formula:

Jitter Statistical = SquareRootOf(SumOf((ElapsedTime[i]-Average)^2)/(ReceivedPacketCount-1))

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Ping Jitter Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Ping Count	Define the number of pings that will be sent. Please enter an integer value.

© 2011 Paessler AG

Sensor Settings	
Timeout (sec.)	Enter a timeout in seconds for the complete request. If the reply takes longer than this value the request is aborted and an error message is triggered. Please enter an integer value.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.49 Ping with Delayed Up Sensor

The Ping with Delayed Up sensor performs a Ping to monitor the availability of a device. It shows the Ping and execution time. As a special feature, you can prolong the time until the sensor switches to an **OK** status after it was **Down**, as the basic Ping Sensor 452 usually responds before many services do.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Usage

The main purpose of this sensor is to use it for monitoring computers in combination with Dependencies 85: If you set this sensor as **Master object for parent**, the device this sensor is created on will be paused while there is no answer received to a Ping request, for example, while a monitored server is restarted (the sensor will show a **Down** status in this case). When a Ping is answered again, for example, after a server restart is completed, you can allow additional time for all services to start on the computer by prolonging the time until the sensor shows an **OK** status again and PRTG resumes monitoring the paused device.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Ping with Delayed Up Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Sensor stays down for	Define the time in seconds that will be waited between first Ping re-received and **OK** status shown after sensor was **Down**.
Ping Timeout	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered. Please enter an integer value.
Buffer Size	Define the buffer size in bytes. Please enter an integer value or leave the field empty. If the field is empty, default value **32** will be used.
Time to Live	Define the TTL value for the ping. Please enter an integer value or leave the field empty. If the field is empty, default value **64** will be used.
Timeout (sec.)	Define the timeout for the internal process. It will be killed if it has not returned a result after this time. Please enter an integer value.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.50 POP3 Sensor

The POP3 sensor monitors a mail server using Post Office Protocol version 3 (POP3). It shows the response time of the server.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

POP3 Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Pop3 Specific	
Timeout	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Specify the port that will be used for the POP3 connection. For non-secure connections usually port 110 is used; usually port 995 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
Transport-Level Security (TLS)	This field is only visible if an option with login is selected above. Choose between: • **Use TLS**: Use a secure connection for the login selected above. • **No encryption (use plain text)**: Use a plain text connection without encryption.

© 2011 Paessler AG

SSL-Method	This field is only visible when TLS is enabled above. Select the SSL method that will be used when connecting to the SMTP server. We recommend using the default value. Only if you experience connection problems, try another setting.

Pop3 Authorisation	
POP3 Authentication Type	Select the kind of authentication for the POP3 connection. Choose between: • **Without Login**: Monitor the connection to the POP3 server only. • **Username and Password**: Log into the POP3 server with user name and password (simple login, non-secure). • **128-bit MD5 hash value (APOP)**: Send the password in an encrypted form using APOP. This option must be supported by the POP3 server you're connecting to.
Username	This field is only visible if an option with login is selected above. Enter a username for POP3 authentication. Please enter a string.
Password	This field is only visible if an option with login is selected above. Enter a password for POP3 authentication. Please enter a string.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.51 POP3 Email Count Sensor

The POP3 Email Count sensor connects to a POP3 email account and returns the number of emails stored in it. Additionally, you can filter by *to* or *from* address, or by *subject*, to only count mails matching the search pattern.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

POP3 Email Count Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Username	Define the username of the POP3 account you want to log into. *Note:* As POP3 server, this sensor will use the parent device's **IP Address/DNS Name** value.
Password	Define the passwort for the POP3 account. *Note:* As POP3 server, this sensor will use the parent device's **IP Address/DNS Name** value.
Mailserver POP3 Port	Define the port number the POP3 server is running at. Please enter an integer value. *Note:* As POP3 server, this sensor will use the parent device's **IP Address/DNS Name** value.

Sensor Settings	
Use SSL	Define whether to use SSL for the connection to the POP3 server. Choose between: ▪ **No** ▪ **Yes** *Note:* As POP3 server, this sensor will use the parent device's hostname.
Filter To Address	Optionally define a *To* address. Only mails containing this will be counted by the sensor. Please enter a string or leave the field empty.
Filter From Address	Optionally define a *From* address. Only mails containing this will be counted by the sensor. Please enter a string or leave the field empty.
Filter Subject Content	Optionally define an email *Subject*. Only mails containing this will be counted by the sensor. Please enter a string or leave the field empty.
Timeout (sec.)	Enter a timeout in seconds for the complete request. If the reply takes longer than this value the request is aborted and an error message is triggered. Please enter an integer value.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.52 Port Sensor

The Port sensor monitors a network service by connecting to its port. It tries to connect to the specified TCP/IP port number of a device and waits for the request to be accepted.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Port Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Ping Settings	
Timeout (sec.)	Enter a timeout in seconds for the port connect. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Enter the number of the port the sensor will try to connect to. Please enter an integer value.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.53 QoS (Quality of Service) Sensor

The QoS (Quality of Service) sensor monitors Voice over IP (VoIP) relevant network parameters by testing network connection quality between two probes. It sends a series of UDP packets from the parent probe to another probe and measures packet loss, jitter, Packet Delay Variation (PDV), etc.

Note: In order for this sensor to work, there has to be at least one remote probe 986 configured in your setup. The sensor can be created on the **Probe Device** of either a local or remote probe.

For a general introduction to the technology behind Quality of Service monitoring, please see **Monitoring Quality of Service** 947 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

QoS (Quality of Service) Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Quality of Service Measurement	
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Target Probe	Define the target probe that will receive the UDP packets. In the drop down menu, all local and remote probes of your setup are shown. When running the sensor on the local probe, select a remote probe as **Target Probe**; if no remote probe is available, please install and connect a remote probe 986 first. When running the sensor on a remote probe, select either another remote probe or the local probe as target. The sensor will measure values for the network track between the probe the sensor is created on and the target probe. *Note:* You must ensure that firewalls, NAT rules, etc. will allow the UDP packets to reach the target probe. The Windows firewall on the target system will be automatically opened by the probe.
Target IP	Define the IP address of the target probe to which the probe the sensor is created on will connect. When you're not using NAT rules, this is usually the address shown above next to the target probe's name.
Port	Define the port on which the UDP packets are sent. Please use a different port for each QoS sensor to make sure packets can be assigned correctly. Enter an integer value between *1024* and *65536*. *Note:* This port must be available on the system running the target probe.
Number of Packets	Define how many packets are sent for each scanning interval. We recommend using **1000**. Please enter an integer value.
Size of Packets (Bytes)	Define the size in bytes of the packets sent. We recommend using **172**. Please enter an integer value.
Time between packets (ms)	Define the size in milliseconds that will be waited between two packets. We recommend using **20**. Please enter an integer value.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).

© 2011 Paessler AG

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.54 RADIUS Sensor

The RADIUS sensor monitors a Remote Authentication Dial-In User Service (RADIUS) server. The sensor tries to authenticate at the server and shows the response time. If authentication fails, it will show an error.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

RADIUS Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Radius specific	
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
User	Define the user name used for authentication at the server. Please enter a string.
Password	Define the password used for authentication at the server. Please enter a string.
Secret	Define the shared secret used for authentication at the server. Please enter a string.
Port	Enter the port number used for connection to the server. Default value is **1812**. Please enter an integer value.
NAS IP Address	Define a valid NAS IP address or leave the field empty.
NAS-Identifier	Enter a NAS identifier. Please enter a string or leave the field empty.
Use Chap	Add a check mark if you want to use the challenge handshake authentication protocol.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.55 RDP (Remote Desktop) Sensor

The RDP (Remote Desktop) Sensor monitors remote desktop services (RDP, Terminal Services Client).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

RDP (Remote Desktop) Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Specific	
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Enter the number of the port the sensor will try to connect to. Please enter an integer value. We recommend using the default value.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.56 Sensor Factory Sensor

The Sensor Factory sensor is a powerful tool that allows you to create your own sensor with channels based on data from other sensors. You can define one or more channels using formulas that combine monitoring results from other sensors.

Samples for usage are:

- Show two or more channels from one or more sensors in one graph.
- Add the value from two or more channels from one or more sensors into a new value (you can also subtract, multiply and divide values).
- Create graphs with one or more graph lines and one or more horizontal lines at specific vertical positions.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Factory Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Factory Specific Settings	
Channel Definition	Enter a channel definition for the sensor. Using a specific syntax, you can refer to data from other sensors here. Please see section Channel Definition Basic Syntax 500 below.
Error Handling	Define the sensor's behavior if one of the sensors defined above is in an error state. In this case, you can set the sensor factory sensor either to error or to warning state. Choose between: • **Factory sensor shows error state when one or more source sensors are in error state** • **Factory sensor shows warning state when one or more source sensors are in error state**

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channel Definition Basic Syntax

The behaviour of a Sensor Factory sensor is controlled by a text field called **Channel Definition**. The basic syntax for a channel definition looks like this:

```
#<id>:<name>[<unit>]
<formula>
```

For each channel one section is used. A section begins with the # sign. Here is an example with two channels:

```
#1:Sample
Channel(1000,0)
#2:Response Time[ms]
Channel(1001,1)
```

The parameters are:

- **<id>** must be a unique number (1 or greater).
- **<name>** is the name of the channel (displayed in graphs and tables).

© 2011 Paessler AG

- **[<unit>]** is optional (e.g. bytes). If it is not provided a fitting unit string is automatically selected (recommended).
- **<formula>** contains the formula to calculate the channel.

In the formula the following elements are allowed:

- Basic operations: **+ - * /**
  Example: *3 + 5 * 2*
- Brackets: **( )**
  Example: *3 * (2 + 6)*
- Compare: **=** (equal), **<>** (not equal), **>** (greater), **<** (less), **>=** (greater or equal), **<=** (less or equal)
  If the compare is true the value is *1*, otherwise *0*. For delta sensors the speed is compared.
- Functions: **channel**, **min**, **max**, **avg**, **percent**

channel() Function

The **channel()** function allows to read the data from a channel of a different sensor. The syntax is:

```
channel(<SensorId>,<ChannelId>)
```

- The **SensorId** is displayed on the sensor details page, in the **Overview** tab behind the sensor name.
- The **ChannelID** is displayed on the sensor details page, in the **Channels** tab for each channel behind the channel name.

Example: Read the data of sensor ID *2001*, channel ID *2*:

```
channel(2001,2)
```

Channels can be gauge values (e.g. Ping ms) or delta values (e.g. traffic kbit/s). Not all combinations are allowed in a formula. *Note:* When performing percentage calculation, please use the **percent() Function** 502 to make sure you obtain the expected values!

There are calculations you *cannot* do:

- You cannot add/subtract a delta from a gauge channel (and vice versa).
- You cannot multiply two delta channels.
- You cannot compare a delta with a gauge channel.
- You cannot use a channel of (another) Sensor Factory sensor channel in the formula.

min() and max() Functions

The **min()** and **max()** functions return the minimum or maximum of the two values. The syntax is:

```
min(<a>,<b>)
max(<a>,<b>)
```

Values for **a** and **b** are either numbers or **channel()** functions, see this example:

```
min(10,5)
min(channel(2001,1),channel(2002,1))
```

The first one returns *5*, the latter one returns the minimum of channel *1* of the sensors with IDs *2001* and *2002*.

© 2011 Paessler AG

avg() Function

The **avg()** function returns the average of the two values. This equals: *(a+b) / 2*. The syntax is:

```
avg(<a>,<b>)
```

Example:

```
avg(20,10)
```

This function returns *15*.

percent() Function

The **percent()** function calculates the percent value of two given values, for example, a channel and a fixed value. The syntax is:

```
percent(<source>,<maximum>[,<unit>])
```

Source is the value the percent is calculated for. This is usually a **channel()** function. **Maximum** is the limit value used for the percent calculation. PRTG will calculate *<source>/<maximum> * 100*.

Unit is optional and is the unit the maximum is provided in. You can use constants with this function (see **Constants** 502 section below for a list). This can be used for gauge (e.g. Ping sensors) and delta (e. g. Traffic Sensors).

The following example shows how to display a traffic sensor as % of maximum bandwidth (100 kilobit/ second):

```
#1:Usage IN
percent(channel(2001,0),100,kilobit)
#2:Usage OUT
percent(channel(2001,1),100,kilobit)
```

Another example shows how to display the values of a sensor as percentage of 200ms:

```
#1:Ping %
percent(channel(2002,0),200)
```

Horizontal Lines

You can add lines to the graph using a formula without a **channel()** function (returning a fixed value). In this case you have to provide the unit of the axis the line is used for. You can use constants here. Examples:

```
#1:Line at 100ms [ms]
100
#2:Line at 50 kbit [kbit/s]
50
#3:2 Mbit/s [kbit/s]
2000
```

Constants

The following constants are defined and can be used in calculations:

- **one** = 1

© 2011 Paessler AG

- **kilo** = 1000
- **mega** = 1000 * kilo
- **giga** = 1000 * mega
- **tera** = 1000 * giga
- **byte** = 1
- **kilobyte** = 1024
- **megabyte** = 1024 * kilobyte
- **gigabyte** = 1024 * megabyte
- **terabyte** = 1024 * gigabyte
- **bit** = 1/8
- **kilobit** = kilo / 8
- **megabit** = mega / 8
- **gigabit** = giga / 8
- **terabit** = tera / 8

More

Knowledge Base: Can I add sensors to Sensor Factory sensors using tags?
- http://www.paessler.com/knowledgebase/en/topic/5143

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.57 sFlow Sensor

The sFlow sensor receives traffic data from a sFlow V5 compatible device and shows the traffic by type. Only header traffic will be analyzed. Please make sure the device matches the sFlow version V5! There are several filter options available to divide traffic into different channels.

Note: In order for the sensor to work, sFlow V5 export must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).

For a general introduction to the technology behind flow monitoring, please see **Monitoring Bandwidth via Flows** 942 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

sFlow Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

sFlow Specific Settings	
Receive sFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the sFlow export options of your hardware router device. Default value is **6343**. Please enter an integer value. Please use a different port for each sFlow device, as traffic is distinguished by port, not by IP address! *Note:* When configuring export, please make sure you select the appropriate sFlow version 5.

© 2011 Paessler AG

sFlow Specific Settings	
Receive sFlow Packets on IP	Select the IP address(es) on which PRTG listens to sFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the sFlow export options of your hardware router device. *Note:* When configuring export, please make sure you select the appropriate sFlow version 5.
Channel Configuration	
Channel Selection	Define the categories the traffic will be accounted to. There are different groups of traffic available. Choose between: ▪ **Web**: Internet web traffic. ▪ **File Transfer**: Traffic caused by FTP. ▪ **Mail**: Internet mail traffic. ▪ **Chat**: Traffic caused by chat and instant messaging. ▪ **Remote Control**: Traffic caused by remote control applications, such as RDP, SSH, Telnet, VNC. ▪ **Infrastructure**: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, SNMP. ▪ **NetBIOS**: Traffic caused by NetBIOS communication. ▪ **Other Protocols**: Traffic caused by various other protocols via UDP and TCP. For each traffic group, you can select how many channels will be used for each group, i.e. how detailed traffic will be divided. For each group, choose between: ▪ **No**: Do not account traffic of this group in an own channel. All traffic of this group will be accounted to the default channel named **Other**. ▪ **Yes**: Count all traffic of this group and summarize it into one channel. ▪ **Detail**: Count all traffic of this group and further divide it into different channels. The traffic will appear in several channels as shown in the **Content** column. *Note:* Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyse.
Filtering	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps and initially when selecting the **Toplists** tab. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ *[Any custom toplists you have added]*

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Toplists

For all xFlow and packet sniffer sensors, there is a **Toplists** tab available. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see Toplists 807 section.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

© 2011 Paessler AG

Others

For more general information about settings, please see Object Settings 111 section.

Related Topics

- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Channel Defintions for xFlow and Packet Sniffer Sensors 982

6.7.58 sFlow (Custom) Sensor

The sFlow (Custom) sensor receives traffic data from a sFlow V5 compatible device and shows the traffic by type. Please make sure the device matches the sFlow version V5! There are several filter options available to divide traffic into different channels.

Note: In order for the sensor to work, sFlow V5 export must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).

For a general introduction to the technology behind flow monitoring, please see **Monitoring Bandwidth via Flows** 942 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

sFlow (Custom) Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

sFlow Specific Settings	
Receive sFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the sFlow export options of your hardware router device. Default value is **6343**. Please enter an integer value. Please use a different port for each sFlow device, as traffic is distinguished by port, not by IP address! *Note:* When configuring export, please make sure you select the appropriate sFlow version 5.

© 2011 Paessler AG

sFlow Specific Settings	
Receive sFlow Packets on IP	Select the IP address(es) on which PRTG listens to sFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the sFlow export options of your hardware router device. *Note:* When configuring export, please make sure you select the appropriate sFlow version 5.
Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see Channel Defintions for xFlow and Packet Sniffer Sensors 982 section. All traffic for which no channel is defined will be accounted to the default channel named **Other**. *Note:* Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyse.
Filtering	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Exclude Filter	First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors 980 section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps and initially when selecting the **Toplists** tab. Choose from: ▪ **Top Talkers** ▪ **Top Connections** ▪ **Top Protocols** ▪ *[Any custom toplists you have added]*

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Toplists

For all xFlow and packet sniffer sensors, there is a **Toplists** tab available. Using toplists, you can review traffic data of small time periods in great detail. For more information, please see Toplists 807 section.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

© 2011 Paessler AG

Others

For more general information about settings, please see Object Settings 111 section.

Related Topics

- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Channel Defintions for xFlow and Packet Sniffer Sensors 982

6.7.59 Share Disk Free Sensor

The Share Disk Free sensor monitors free disk space of a share (Windows/Samba) using Server Message Block (SMB). It shows the free space in percent and total.

Note: This sensor only works if no quotas are enabled on the target share. If there are quotas enabled for the user account this sensor uses to connect to the share, the absolute value will be okay, but the percentage variable will show wrong values.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Share Disk Free Sensor

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Share Configuration	
Share	Enter the name of the share this sensor will monitor. Only a share name is allowed here (for example **C$**). Please do not enter a complete UNC name here. The server name is taken from the parent device of this sensor.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.

© 2011 Paessler AG

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.60 SMTP Sensor

The SMTP sensor monitors a mail server using Simple Mail Transfer Protocol (SMTP) and shows the server's response time. It can optionally send a test email with every check.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

SMTP Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SMTP specific	
Timeout (sec)	Enter a timeout in seconds for the SMTP connect. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Enter the number of the port that will be used to send an email via SMTP. For non-secure connections usually port 25 is used; usually port 465 or 587 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
TLS (Transport-Level Security)	Select if the SMTP connection will be secured via SSL. Choose between: • **Don't use**: Do not use encryption for the SMTP connection. • **Use**: Connect to the SMTP server using the SSL method selected below.

SSL-Method	This field is only visible when TLS is enabled above. Select the SSL method that will be used when connecting to the SMTP server. We recommend using the default value. Only if you experience connection problems, try another setting.

Authentication	
Type	Select the kind of authentication for the SMTP connection. Choose between: • **None**: Do not use any authentication method. • **Username/Password**: Authenticate at the SMTP server via username and password.
Username	This field is only visible if SMTP authentication is enabled above. Enter a username for SMTP authentication. Please enter a string.
Password	This field is only visible if SMTP authentication is enabled above. Enter a password for SMTP authentication. Please enter a string.

Monitoring	
Send Mail	Define if an email will be sent when connecting to the SMTP server. Choose between: • **None**: Do not send an email, just connect to the SMTP server. • **Send Mail**: Send an email through the SMTP server. If there is an error when sending mail, an error message will be triggered and the sensor will be put in a down state.
Helo Ident	Enter a server name for the helo part of the mail protocol. For some mail servers the helo ident must be the valid principal host domain name for the client host.
From	Specify which address the sent emails will contain in the from field. Please enter a valid email address.
To	Specify to which address the emails will be sent to. Please enter a valid email address.
Topic	Specify which subject will be used in the sent emails. Please enter a string or leave the field empty.
Content	Specify which body will be used in the sent emails. Please enter a string or leave the field empty.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor.

© 2011 Paessler AG

Sensor Display	
	▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.61 SMTP&IMAP Round Trip Sensor

SMTP&IMAP Round Trip sensor monitors the time it takes for an email to reach an Internet Message Access Protocol (IMAP) mailbox after being sent using Simple Mail Transfer Protocol (SMTP). It sends an email to the parent device via SMTP and then checks an IMAP mailbox until the email comes in. The sensor shows the response time of SMTP and IMAP server, and the sum of both.

For a general introduction to the technology behind round trip monitoring, please see **Monitoring Email Round Trip** 951 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

We recommend adding this sensor on an SMTP server device only, as the sensor's settings are optimized for this scenario.

SMTP&IMAP Round Trip Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Email Settings	
From	Specify which address the sent emails will contain in the from field. Please enter a valid email address.
To	Specify to which address the emails will be sent to. Please enter a valid email address.
Helo Ident	Enter a server name for the helo part of the mail protocol. For some mail servers the helo ident must be the valid principal host domain name for the client host.

Step 1: Send email to parent device using SMTP	
In this step, you configure how emails will be sent. As SMTP server, the sensor uses the **IP-Address/DNS Name** property's value of the device it is added on.	
Port	Enter the number of the port that will be used to send an email via SMTP. Please enter an integer value. For non-secure connections usually port 25 is used; usually port 465 or 587 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
Timeout for SMTP Connection (sec)	Enter a timeout in seconds for the SMTP connect. If the reply takes longer than this value the request is aborted and an error message is triggered.
SMTP Authentication Type	Select the kind of authentication for the SMTP connection. Choose between: • **None**: Do not use any authentication method. • **Username/Password**: Authenticate at the SMTP server via username and password.
Username	This field is only visible if SMTP authentication is enabled above. Enter a username for SMTP authentication. Please enter a string.
Password	This field is only visible if SMTP authentication is enabled above. Enter a password for SMTP authentication. Please enter a string.
TLS (Transport-Level Security)	Select if the SMTP connection will be secured via SSL. Choose between: • **Don't use**: Do not use encryption for the SMTP connection. • **Use**: Connect to the SMTP server using the SSL method selected below.
SSL-Method	This field is only visible when TLS is enabled above. Select the SSL method that will be used when connecting to the SMTP server. We recommend using the default value. Only if you experience connection problems, try another setting.

© 2011 Paessler AG

Step 2: Check an IMAP mailbox until email arrives	
In this step, you configure how the sent emails will be received.	
IP-Address/DNS Name	Specify the IMAP server. Enter a valid IP address or DNS name.
Mailbox	Specify the IMAP Mailbox (resp. "IMAP folder") you want to check. Please enter the IMAP mailbox/folder name.
Port	Specify the port that will be used for the IMAP connection. For non-secure connections usually port 143 is used; usually port 993 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
TLS (Transport-Level Security)	Select if the IMAP connection will be secured via SSL. Choose between: • **Don't use**: Do not use encryption for the SMTP connection. • **Use**: Connect to the SMTP server using the SSL method selected below.
SSL-Method	This field is only visible when TLS is enabled above. Select the SSL method that will be used when connecting to the IMAP server. We recommend using the default value. If you experience connection problems, try another setting.
Connection Interval (sec)	Enter the number of seconds the sensor will wait between two connections to the IMAP server. PRTG will repeatedly check the mailbox in this interval until the email arrives. Please enter an integer value.
Maximum Trip Time (sec)	Enter the number of seconds an email may take to arrive in the IMAP mailbox. PRTG will repeatedly check the mailbox in the interval specified above until the email arrives. If it does not arrive within the maximum trip time, an error message will be triggered for the sensor. Please enter an integer value.
IMAP Authentication Type	Select the kind of authentication for the IMAP connection. Choose between: • **Username and Password (simple)** • **Simple Authentication and Security Layer (SASL)**
Username	Enter a username for IMAP authentication. Please enter a string.
Password	Enter a username for IMAP authentication. Please enter a string.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.62 SMTP&POP3 Round Trip Sensor

SMTP&POP3 Round Trip sensor monitors the time it takes for an email to reach an Post Office Protocol version 3 (POP3) mailbox after being sent using Simple Mail Transfer Protocol (SMTP). It sends an email to the parent device via SMTP and then checks a POP3 mailbox until the email comes in. The sensor shows the response time of SMTP and POP3 server, and the sum of both.

For a general introduction to the technology behind round trip monitoring, please see **Monitoring Email Round Trip** 951 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

We recommend adding this sensor on an SMTP server device only, as the sensor's settings are optimized for this scenario.

SMTP&POP3 Round Trip Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

Email Settings	
From	Specify which address the sent emails will contain in the from field. Please enter a valid email address.
To	Specify to which address the emails will be sent to. Please enter a valid email address.
Helo Ident	Enter a server name for the helo part of the mail protocol. For some mail servers the helo ident must be the valid principal host domain name for the client host.

Step 1: Send email to parent device using SMTP	
In this step, you configure how emails will be sent. As SMTP server, the sensor uses the **IP-Address/DNS Name** property's value of the device it is added on.	
Port	Enter the number of the port that will be used to send an email via SMTP. Please enter an integer value. For non-secure connections usually port 25 is used; usually port 465 or 587 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
Timeout for SMTP Connection (sec)	Enter a timeout in seconds for the SMTP connect. If the reply takes longer than this value the request is aborted and an error message is triggered.
TLS (Transport-Level Security)	Select if the SMTP connection will be secured via SSL. Choose between: • **Don't use**: Do not use encryption for the SMTP connection. • **Use**: Connect to the SMTP server using the SSL method selected below.
SSL-Method	This field is only visible when TLS is enabled above. Select the SSL method that will be used when connecting to the SMTP server. We recommend using the default value. Only if you experience connection problems, try another setting.
SMTP Authentication Type	Select the kind of authentication for the SMTP connection. Choose between: • **None**: Do not use any authentication method. • **Username/Password**: Authenticate at the SMTP server via username and password.
Username	This field is only visible if SMTP authentication is enabled above. Enter a username for SMTP authentication. Please enter a string.
Password	This field is only visible if SMTP authentication is enabled above. Enter a password for SMTP authentication. Please enter a string.

Step 2: Check a POP3 mailbox until email arrives	
In this step, you configure how the sent emails will be received.	
IP-Address/DNS Name	Specify the POP3 server. Enter a valid IP address or DNS name.
Port	Specify the port that will be used for the POP3 connection. For non-secure connections usually port 110 is used; usually port 995 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
TLS (Transport-Level Security)	Select if the POP3 connection will be secured via SSL. Choose between: • **Don't use**: Do not use encryption for the SMTP connection. • **Use**: Connect to the SMTP server using the SSL method selected below.
SSL-Method	This field is only visible when TLS is enabled above. Select the SSL method that will be used when connecting to the IMAP server. We recommend using the default value. If you experience connection problems, try another setting.
Connection Interval (sec)	Enter the number of seconds the sensor will wait between two connections to the IMAP server. PRTG will repeatedly check the mailbox in this interval until the email arrives. Please enter an integer value.
Maximum Trip Time (sec)	Enter the number of seconds an email may take to arrive in the IMAP mailbox. PRTG will repeatedly check the mailbox in the interval specified above until the email arrives. If it does not arrive within the maximum trip time, an error message will be triggered for the sensor. Please enter an integer value.
POP3 Authentication Type	Select the kind of authentication for the POP3 connection. Choose between: • **Without Login**: Monitor the connection to the POP3 server only. • **Username and Password**: Log into the POP3 server with user name and password (simple login, non-secure). • **128-bit MD5 hash value (APOP)**: Send the password in an encrypted form using APOP. This option must be supported by the POP3 server you're connecting to.
Username	This field is only visible if an option with login is selected above. Enter a username for POP3 authentication. Please enter a string.
Password	This field is only visible if an option with login is selected above. Enter a username for POP3 authentication. Please enter a string.

© 2011 Paessler AG

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.63 SNMP Custom Sensor

Monitors a numerical value returned by a specific OID using Simple Network Management Protocol (SNMP).

For a general introduction to the technology behind SNMP, please see **Monitoring via SNMP** 935 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

OID values	
Channel Name	Enter a name for the channel the results at the given OID will be will shown in. You can change this value later in the sensor's channel settings 792.
Value Type	Select how the results at the given OID will be handled. Choose between: ▪ **Gauge (unsigned Integer)**: For integer values, such as *10* or *120*. ▪ **Gauge (signed integer)**: For integer values, such as *-12* or *120*. ▪ **Gauge (float)**: For float values, such as *-5.80* or *8.23*. ▪ **Delta (Counter)**: For counter values. PRTG will calculate the difference between the last and the current value. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SNMP Custom Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.

© 2011 Paessler AG

Basic Sensor Settings	
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

OID values	
OID value	Enter the OID of the SNMP object you want to receive numerical data from.
Unit String	Define the unit of the numerical data that will be received at the given OID. Please enter a string.
Value Type	Shows the value type of the numerical data that will be received at the given OID.Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Multiplication	If you want to multiply the received data with a certain value, enter the quotient here. Please enter an integer or float value.
Division	If you want to divide the received data by a certain value, enter the divisor here. Please enter an integer or float value.
If value changes	Define what shall be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change. • **Trigger 'On Change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.64 SNMP Custom String Sensor

The SNMP Custom String sensor monitors a string returned by a specific OID using Simple Network Management Protocol (SNMP).

For a general introduction to the technology behind SNMP, please see **Monitoring via SNMP** 935 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

SNMP Custom String Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

OID values	
OID value	Enter the OID of the SNMP object you want to receive a string from.
If value changes	Define what shall be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change. • **Trigger 'On Change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.
Response must include	Define which string must be part of the data that will be received from the SNMP object at the given OID. If the data does not include this string, the sensor will be set to an error state. Please enter a string value or leave the field empty.
Response must not include	Define which string must not be part of the data that will be received from the SNMP object at the given OID. If the data does include this string, the sensor will be set to an error state. Please enter a string value or leave the field empty.
Minimum length of string	Define the minimum length of the string that will be received from the SNMP object at the given OID. If the length is less than this value, the sensor will be set to an error state. Please enter an integer value or leave the field empty.
Maximum length of string	Define the maximum length of the string that will be received from the SNMP object at the given OID. If the length is greater than this value, the sensor will be set to an error state. Please enter an integer value or leave the field empty.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.65 SNMP Library Sensor

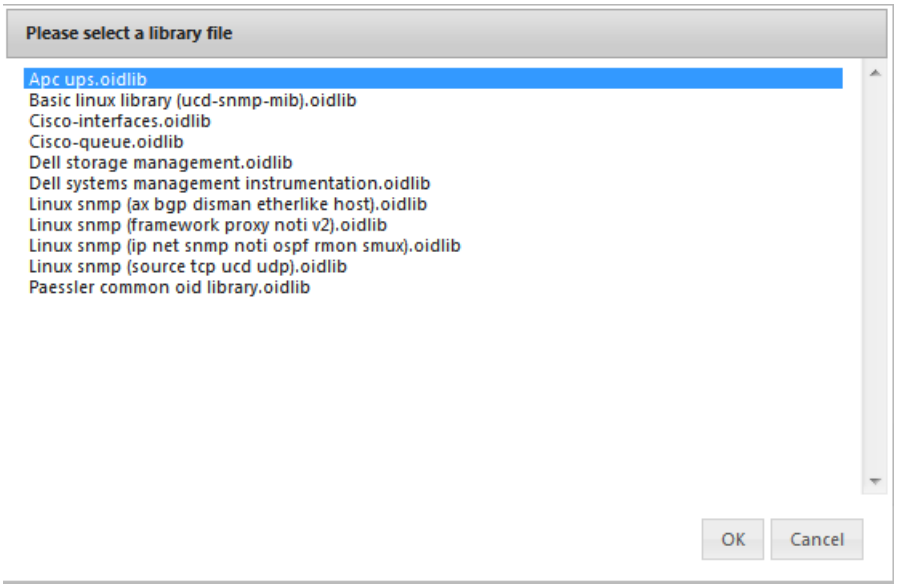
The SNMP Library sensor monitors a device using Simple Network Management Protocol (SNMP) in combination with a compiled Management Information Base (MIB) library file. This provides extended monitoring beyond other the SNMP sensors of PRTG.

In order to monitor any SNMP capable device, you can download the manufacturer's MIB files for these devices, convert them to the Paessler *oidlib* format and import them into PRTG. To make your monitoring setup as convienient as possible, PRTG is delivered with pre-compiled *oidlib* library files that already contain the Object Identifier (OID) of SNMP counters for the most common devices in a network.

For a general introduction to the technology behind SNMP, please see Monitoring via SNMP 935 section.

Add Sensor

Manually add 165 a new sensor to an SNMP device and from the **Add Sensor** dialog, select **SNMP Library** sensor. PRTG will show a list of *oidlib* files available on the system. This contains all library files stored at the *\PRTG Network Monitor\snmplibs* sub-directory of your PRTG installation—both the ones delivered with PRTG and your own files.



List of SNMP Default Library Files

The file names in the list indicate the potential purpose. Select a name that appears appropriate for your device and confirm with the **OK** button. Often, **Paessler common oid library.oidlib** is a good start. If the file does not fit to your device, this will result in an error message saying that no available interfaces were found on this device. If you see this message, please hit the **Go back and retry** button and try with another file. If counters were found for your device, you will see the sensor's settings.

Default OIDLIB Files Overview

The following files are delivered with PRTG and allow to extend your SNMP monitoring for many devices. Please be aware that not all devices and/or parameters may be supported by the libraries.

- **APC UPS.oidlib**
  Can be used to monitor uninterruptible power supplies (UPS) from APC American Power Conversion Corp.

- **Basic Linux Library (UCD-SNMP-MIB).oidlib**
  Can be used to monitor basic system parameters on Linux systems, such as memory, disk and swap, CPU, etc.

- **cisco-interfaces.oidlib**
  Can be used to monitor Cisco specific parameters.

- **cisco-queue.oidlib**
  Can be used to monitor Cisco specific parameters.

- **Dell Storage Management.oidlib**
  Can be used to monitor Dell storage devices. Possible parameters include disk arrays, battery and power supply, fan and temperature, virtual disk, etc.

- **Dell Systems Management Instrumentation.oidlib**
  Can be used to monitor the hardware of Dell systems. Possible parameters include ACPower and battery, alerts, base board, Bios, BMC, chassis, COO, cooling, event log, firmware, IDE, keyboard, memory, port, network, processor, SCSI, system, temperature, USB, UUID, etc.

- **Linux SNMP (AX BGP DisMan EtherLike Host).oidlib**
  Can be used to monitor different aspects of Linux systems. *Note:* This file can find a very large number of possible interfaces. It may take a few seconds until the selection table is shown.

- **Linux SNMP (Framework Proxy Noti v2).oidlib**
  Can be used to monitor different aspects of Linux systems. *Note:* This file can find a very large number of possible interfaces. It may take a few seconds until the selection table is shown.

- **Linux SNMP (IP Net SNMP Noti OSPF RMON SMUX).oidlib**
  Can be used to monitor different aspects of Linux systems. *Note:* This file can find a very large number of possible interfaces. It may take a few seconds until the selection table is shown.

- **Linux SNMP (Source TCP UCD UDP).oidlib**
  Can be used to monitor different aspects of Linux systems. *Note:* This file can find a very large number of possible interfaces. It may take a few seconds until the selection table is shown.

- **Paessler Common OID Library.oidlib**
  Can be used to monitor many common hardware devices.

© 2011 Paessler AG

Import MIB Files

Additionally you can create your own *oidlib* files by importing your device manufacturers' MIB files, using a the free Paessler **MIB Importer**. For more information and download, please see the link in the More 556 section below.

SNMP Library Sensor—Add Sensor Settings

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

SNMP Library Specific	
Library	This shows the path to the *oidlib* file selected before. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Library-OIDs	Select the aspects of the device you want to monitor. A list specific to your setup is shown. It contains all counters found in the chosen library that match your device. Select one or more items by adding a check mark in front of the respective line. For each selection one sensor will be created when you click the **Continue** button.

SNMP Library Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SNMP Library Specific	
Selected Interface	Shows the interface monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Unit String	Enter a string describing the unit of the returned values. This is for display purposes only. Please enter a string.
Multiplication	If you want to multiply the received data with a certain value, enter the quotient here. Please enter an integer or float value, or leave the field empty.
Division	If you want to divide the received data by a certain value, enter the divisor here. Please enter an integer or float value, or leave the field empty.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I import my MIB files into PRTG?
- http://www.paessler.com/knowledgebase/en/topic/733

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

© 2011 Paessler AG

Others

For more general information about settings, please see Object Settings 111 section.

6.7.66 SNMP Linux Disk Free Sensor

The SNMP Disk Free sensor monitors free space on disks of a Linux/Unix system using Simple Network Management Protocol (SNMP). It shows the total free disk space (sum), and the free disk space in percent for every mounted partition (volume).

For a general introduction to the technology behind SNMP, please see **Monitoring via SNMP** 935 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

SNMP Disk Free Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.67 SNMP Linux Load Average Sensor

The SNMP Load Average sensor monitors the system load average of a Linux/Unix system using Simple Network Management Protocol (SNMP). It shows the average system load within a one, five, and 15 minutes interval (each in one channel).

For a general introduction to the technology behind SNMP, please see **Monitoring via SNMP** 935 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

SNMP Load Average Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.68 SNMP Linux Meminfo Sensor

The SNMP Load Average sensor monitors the memory usage of a Linux/Unix system using Simple Network Management Protocol (SNMP). It shows the available memory in total and in percent.

For a general introduction to the technology behind SNMP, please see **Monitoring via SNMP** 935 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

SNMP Meminfo Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).

© 2011 Paessler AG

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.69 SNMP Traffic Sensor

The SNMP Traffic sensor monitors traffic on a device using Simple Network Management Protocol (SNMP). It can be created on a device which provides traffic data.

For a general introduction to the technology behind SNMP, please see **Monitoring via SNMP** 935 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

For SNMP devices with multiple interfaces multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Traffic specific	
Interface number	Select the interfaces you want to add a sensor for. A list of SNMP device interfaces is shown; containing all interfaces which your device provides. Connected interfaces are printed in bold face; not connected in non-bold face. One sensor will be created for each interface. You can group-select and -unselect interfaces by using the buttons **Select all connected interfaces**, **Select all disconnected interfaces**, and **Deselect all interfaces**.
Description IN	For the standard channel "Traffic In" enter the description here. It will be shown in graphs and tables. You can change this description and the description of all other channels in the sensor's channel settings 792 later.
Description OUT	For the standard channel "Traffic Out" enter the description here. It will be shown in graphs and tables. You can change this description and the description of all other channels in the sensor's channel settings 792 later.
Description SUM	For the standard channel traffic "Sum" enter the description here. It will be shown in graphs and tables. You can change this description and the description of all other channels in the sensor's channel settings 792 later.

SNMP Traffic Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Traffic specific	
Interface number	Shows the number and name of the interface in your physical device that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Additional Channels	By default, the channels "Traffic In" and "Traffic out" are created for each sensor. Choose additional channels for all selected interfaces. Please click on the respective channel name(s); a check mark symbol will appear in front of them. You can choose from the following additional channels: • **Errors In & Out** • **Discards In & Out** • **Unicast Packets In & Out** • **Non Unicast Packets In & Out (32-bit only)** • **Multicast Packets In & Out (64-bit only)** • **Broadcast Packets In & Out (64-bit only)** • **Unknown Protocols** Channels that are once created cannot be deleted later. They can be disabled only.
Connection State Handling	Choose how PRTG will react when an interface is disconnected. A disconnected interface is, for example, an ethernet port on a switch with no cable plugged in. This setting is valid for all interfaces selected above. You can choose between: • **Show alarm when disconnected (recommended)**: The sensor for the interface will turn into a red error state. • **Ignore interface when disconnected**: No alarm will be shown in PRTG; monitoring will be discontinued without notice.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.

© 2011 Paessler AG

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.70 SNMP Trap Receiver Sensor

The SNMP Trap Receiver sensor receives and analyzes Simple Network Management Protocol (SNMP) traps. It returns the number of new traps and the number of warnings, per second.

For a general introduction to the technology behind SNMP, please see **Monitoring via SNMP** 935 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

SNMP Trap Receiver Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

OID values	
OID value	Enter the OID of the SNMP object you want to receive numerical data from.
Listen on port	Define the port on which SNMP traps are received. We recommend using the default value.
When Message comes in	Define what will be done when a message comes in. Choose between: ▪ **Do nothing**: Do not perform any action. • **Write message to log and fire 'change' trigger**: Write an entry to the PRTG log file every time a message is received. *Note:* Use with caution; this may create a lot of log entries!
Sender	Define if you want to filter for a specific sender only. If you enter something here, only traps with this sender will be regarded. Make sure the string matches exactly the value of the sender value in the trap. Please enter a string or leave the field empty.
Specific Trap Code	Define if you want to filter for a specific trap code value only. If you enter something here, only traps with this code will be regarded. Make sure the value matches exactly the code in the trap. Please enter an integer value or leave the field empty.
Set sensor to 'warning'	Define when the sensor will be put to a **Warning** status. Choose between: ▪ **Never**: Never put the sensor to a warning status. ▪ **Depending on Content**: Put the sensor to a warning status, depending on the content of the messages received. Please define below.
Message must include	This setting is only visible if a sensor status change is enabled above. Define which string must be part of the trap's message. If the message does not include this string, the sensor will be set to a **Warning** status. Please enter a string or leave the field empty.
Message must not include	This setting is only visible if a sensor status change is enabled above. Define which string must not be part of the trap's message. If the message does include this string, the sensor will be set to a **Warning** status. Please enter a string or leave the field empty.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I use PRTG's trap receiver and what are its limitations?
- http://www.paessler.com/knowledgebase/en/topic/143

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.71 SNMP Uptime Sensor

The SNMP Uptime sensor monitors the uptime of a device using Simple Network Management Protocol (SNMP). It read a device's value for system uptime and shows it.

For a general introduction to the technology behind SNMP, please see Monitoring via SNMP 935 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

SNMP Uptime Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.72 SSH Disk Free Sensor

The SSH Disk Free sensor monitors free space on disks of a Linux/Unix system using Secure Shell (SSH). It shows the total free disk space (sum), and the free disk space in percent for every mounted partition (volume).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

SSH Disk Free Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SSH Specific	
Connection Timeout (sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. *cat /proc/loadavg*).
Port	Enter the SSH port. Usually, this is port 22.
Result Handling	Define what will be done with the result of the query. Choose between: • **Discard text result**: Do not store the requested web page.

SSH Specific	
	• **Store latest text result**: Store the last result received from the query to the "Logs (System)" directory (on the Master node, if in a cluster). File name: *Result of Sensor [ID].txt*. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **More** 300 section below.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

More

Knowledge Base article: How and Where Does PRTG Store its Data?

- http://www.paessler.com/knowledgebase/en/topic/463

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

© 2011 Paessler AG

Others

For more general information about settings, please see Object Settings 111 section.

6.7.73 SSH INodes Free Sensor

The SSH INodes Free sensor monitors the free index nodes on disks of Linux/Unix and MacOS systems via Secure Shell (SSH). It shows the free index nodes in percent, for each mount in an own sensor channel.

UNIX file systems only allow a limited number of index nodes. If the limit is exceeded, no more data can be stored, although there might be still free space available. This sensor can help you to notice early on if one of your drives is running out of INodes.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

SSH INodes Free Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SSH Specific	
Connection Timeout (sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. *cat /proc/loadavg*).
Port	Enter the SSH port. Usually, this is port 22.
Result Handling	Define what will be done with the result of the query. Choose between: • **Discard text result**: Do not store the requested web page.

© 2011 Paessler AG

SSH Specific	
	• **Store latest text result**: Store the last result received from the query to the "Logs (System)" directory (on the Master node, if in a cluster). File name: *Result of Sensor [ID].txt*. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **More** 300 section below.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

More

Knowledge Base article: How and Where Does PRTG Store its Data?

- http://www.paessler.com/knowledgebase/en/topic/463

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.74 SSH Load Average Sensor

The SSH Load Average sensor monitors the load average of a Linux/Unix system using Secure Shell (SSH). It shows the average system load within a one, five, and 15 minutes interval (each in one channel).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

SSH Load Average Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SSH Specific	
Connection Timeout (sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. *cat /proc/loadavg*).
Port	Enter the SSH port. Usually, this is port 22.
Result Handling	Define what will be done with the result of the query. Choose between: • **Discard text result**: Do not store the requested web page.

SSH Specific	
	• **Store latest text result**: Store the last result received from the query to the "Logs (System)" directory (on the Master node, if in a cluster). File name: *Result of Sensor [ID].txt*. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **More** 300 section below.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

More

Knowledge Base article: How and Where Does PRTG Store its Data?

- http://www.paessler.com/knowledgebase/en/topic/463

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

© 2011 Paessler AG

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.75 SSH Meminfo Sensor

The SSH Meminfo sensor monitors the memory usage of a Linux/Unix system using Secure Shell (SSH). It shows the available memory in total and in percent.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

SSH Meminfo Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SSH Specific	
Connection Timeout (sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. *cat /proc/loadavg*).
Port	Enter the SSH port. Usually, this is port 22.
Result Handling	Define what will be done with the result of the query. Choose between: • **Discard text result**: Do not store the requested web page. • **Store latest text result**: Store the last result received from the query to the "Logs (System)" directory (on the Master node, if in a cluster). File name: *Result of Sensor [ID].txt*. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **More** 300 section below.

© 2011 Paessler AG

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

More

Knowledge Base article: How and Where Does PRTG Store its Data?

- http://www.paessler.com/knowledgebase/en/topic/463

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.76 SSH VMWare ESX(i) Disk Sensor

The SSH VMWare ESX(i) Disk sensor monitors free space on disks of a VMware ESX(i) system using Secure Shell (SSH). It shows the free disk space for different mounts and total, in total and percent values.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

SSH VMWare ESX(i) Disk Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SSH Specific	
Connection Timeout (sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. *cat /proc/loadavg*).
Port	Enter the SSH port. Usually, this is port 22.
Result Handling	Define what will be done with the result of the query. Choose between: • **Discard text result**: Do not store the requested web page.

SSH Specific	
	• **Store latest text result**: Store the last result received from the query to the "Logs (System)" directory (on the Master node, if in a cluster). File name: *Result of Sensor [ID].txt*. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **More** 300 section below.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

More

Knowledge Base article: How and Where Does PRTG Store its Data?

- http://www.paessler.com/knowledgebase/en/topic/463

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

© 2011 Paessler AG

Others

For more general information about settings, please see Object Settings 111 section.

6.7.77 Syslog Receiver Sensor

The Syslog Receiver sensor receives and analyzes Syslog messages. It shows the number of new messages and warnings, per second.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Syslog Receiver Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Syslog Specific	
Listen on port	Enter the port the sensor will listen on for Syslog messages. Usually port 514 is used. Please enter an integer value. We recommend using the default value.
Sender	Enter the sender which the Syslog messages are to come from. Only messages from a sender matching this string will be regarded. If you enter a value here, make sure your entry matches exactly the value for the sender in the Syslog message. Please enter a string or leave the field empty.
When Message comes in	• Define what will be done when a message comes in. Choose between: ▪ **Do nothing**: Do not perform any action.

© 2011 Paessler AG

Syslog Specific	
	• **Write message to log and fire 'change' trigger**: Write an entry to the PRTG log file every time a message is received. *Note:* Use with caution; this may create a lot of log entries!
Set sensor to "warning"	Define which conditions will set the sensor's status to warning. Choose between: • **Never**: The sensor's status will always show ok, no matter if messages are received or not. • **Depending on Severity**: The sensor's status will be set to warning for certain conditions in the Syslog messages. • **Depending on Content**: The sensor's status will be set to warning if the Syslog message does or does not a defined string.
Emergency	This option is only visible if warning depending on severity is enabled above. Set sensor to warning if a Syslog message contains an emergency message.Add a check mark symbol in front of the **Warn on this condition** text to enable this option.
Alert	This option is only visible if warning depending on severity is enabled above. Set sensor to warning if a Syslog message contains an alert message. Add a check mark symbol in front of the **Warn on this condition** text to enable this option.
Critical	This option is only visible if warning depending on severity is enabled above. Set sensor to warning if a Syslog message contains a critical message. Add a check mark symbol in front of the **Warn on this condition** text to enable this option.
Error	This option is only visible if warning depending on severity is enabled above. Set sensor to warning if a Syslog message contains an error message. Add a check mark symbol in front of the **Warn on this condition** text to enable this option.
Warning	This option is only visible if warning depending on severity is enabled above. Set sensor to warning if a Syslog message contains a warning message. Add a check mark symbol in front of the **Warn on this condition** text to enable this option.
Notice	This option is only visible if warning depending on severity is enabled above. Set sensor to warning if a Syslog message contains a notice message. Add a check mark symbol in front of the **Warn on this condition** text to enable this option.
Informational	This option is only visible if warning depending on severity is enabled above. Set sensor to warning if a Syslog message contains an informational message. Add a check mark symbol in front of the **Warn on this condition** text to enable this option.

Syslog Specific	
Message must include	This option is only visible if warning depending on content is enabled above. Define which string must be part of one or more Syslog message(s) received, in order for the sensor to show an ok status. If a message does *not* include this string, the sensor's status will be set to warning. Please enter a string or leave the field empty.
Message must not include	This option is only visible if warning depending on content is enabled above. Define which string must *not* be part of one or more Syslog message(s) received, in order for the sensor to show an ok status. If a message *does* include this string, the sensor's status will be set to warning. Please enter a string or leave the field empty.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.78 TFTP Sensor

The TFTP sensor monitors a Trivial File Transfer Protocol (TFTP) server and checks if a certain file is available for download. It shows the availability.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

TFTP Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Specific	
Timeout (sec)	Enter a timeout in seconds for the TFTP connect. If the reply takes longer than this value the request is aborted and an error message is triggered. Please enter an integer value.
Port	Enter the number of the port the TFTP service is running on. The sensor will try to connect to it. Please enter an integer value.
Filename	Enter the name of the file the sensor will check. If this filename is not available on the server, the sensor's state will be set to down. Please enter a string.

© 2011 Paessler AG

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.79 Traceroute Hop Count Sensor

The Traceroute Hop Count sensor traces the number of hops needed from the probe system the sensor is running on to the **IP Address/DNS Name** defined in the sensor's parent device. It returns the number of hops. In case this number changes, you can additionally change the sensor's status.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Traceroute Hop Count Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
If Route Changes	Define what will be done in case the number of hops has changed since last check. Choose between: ▪ **Ignore**: Do not perform any action. ▪ **Set sensor to "Warning"**: Set the sensor to warning status. ▪ **Set sensor to "Error"**: Set the sensor to error status.
Timeout (sec.)	Define the timeout for the internal process. It will be killed if it has not returned a result after this time. Please enter an integer value.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.80 Virtuozzo Container Disk Sensor

The Virtuozzo Host Server sensor monitors a Parallels™ Virtuozzo host server. This sensor must be created on a Windows server parent device running Virtuozzo. For each container, it can show disk space used (kb-blocks), disk space soft and hard limit (kb-blocks), the number of inodes, and inodes soft and hard limit.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Container Settings	
Container	Select all Containers for which you want to create a sensor for disk monitoring. Select by adding a check mark in front of the respective container name. For each container one sensor will be created. Sensor names are created automatically, based on the container name.

Virtuozzo Container Disk Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Container Settings	
Env ID	Shows the unique ID of the container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

© 2011 Paessler AG

Container Settings	
Name	Shows the name of the monitored container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
OS	Shows the operating system running on the container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows a description for the container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Powered Off Containers	Define if the sensor will go into an error state if the container is powered off. • **Alarm when powered off**: Set the sensor for a container to error if the container is powered off. • **Ignore powered off state**: Only show zero values for a sensor when the monitored container is powered off. Do not set the sensor to error.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.81 Virtuozzo Container Network Sensor

The Virtuozzo Host Server sensor monitors a Parallels™ Virtuozzo host server. This sensor must be created on a Windows server parent device running Virtuozzo. For each container, it can show network usage as incoming and outgoing bytes, and the number of incoming and outgoing packets.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Container Settings	
Container	Select all Containers for which you want to create a sensor for disk monitoring. Select by adding a check mark in front of the respective container name. For each container one sensor will be created. Sensor names are created automatically, based on the container name.

Virtuozzo Container Network Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Container Settings	
Env ID	Shows the unique ID of the container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

© 2011 Paessler AG

Container Settings	
Name	Shows the name of the monitored container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
OS	Shows the operating system running on the container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows a description for the container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Powered Off Containers	Define if the sensor will go into an error state if the container is powered off. • **Alarm when powered off**: Set the sensor for a container to error if the container is powered off. • **Ignore powered off state**: Only show zero values for a sensor when the monitored container is powered off. Do not set the sensor to error.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.82 VMware Host Hardware (WBEM)

The VMware Host Hardware sensor monitors hardware information of a ESX/ESXi server using Web-Based Enterprise Management (WBEM). It shows the current reading and health state.

Note: The parent device must be a VMware ESX/ESXi server (version 3.5 or 4.0) with values set for **Credentials for Linux (WBEM/SSH) Systems**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one elements multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

ESX Server Elements	
ESX Element	You see a list of all available ESX hardware elements on the host server on this device. Please choose one or more elements by adding a check mark in front of the respective line. For each element one sensor will be created.

VMware Host Hardware (WBEM) Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

ESX Server Elements	
Element	Shows the ESX element monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Automatic Sensor State	Define if the sensor will change it's status dependent on the health state reading. Choose between: ▪ **Set sensor state automatically to 'Warning' or 'Down'**: Set the sensor to a **Warning** or **Down** status when the server returns respective values. The sensor will additionally change to a **Down** status if the connection to the server fails. ▪ **Just report the current reading, ignore Server Health Value**: Never change the sensor's status dependent on the values returned by the server. The sensor will only change to a **Down** status if the connection to the server fails.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.83 VMware Host Server (SOAP) Sensor

The VMware Host Server (SOAP) sensor monitors a VMware host server using Simple Object Access Protocol. It shows CPU (percent) and memory (absolute) usage, disk read and write speed, and network received and transmitted speed of a VMware host server.

Note: The parent device must be a VMware ESX/ESXi server (version 3.5 or 4.0).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

VMware Host Server Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.84 VMware Virtual Machine (SOAP) Sensor

The VMware Virtual Machine (SOAP) sensor monitors a virtual machine on a VMware host server using Simple Object Access Protocol. It shows CPU (percent) and memory (absolute) usage, disk read and write speed, and network received and transmitted speed of a single virtual machine.

Note: The parent device must be a VMware ESX/ESXi host server or a Virtual Center server (version 3.5 or 4.0).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Note: PRTG requests a full list of all virtual machines configured on the device. Therefore, it may take a few seconds before the dialog is loaded.

If you select more than one virtual machine multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Virtual Machine Settings	
Virtual Machine	You see a list of all virtual machines (VMs) available on the host server on this device, including the ones that are not running. All VMs are listed with name and the OS it is running on. Please choose one or more machines by adding a check mark in front of the respective line. For each VM one sensor will be created.

VMware Virtual Machine Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.

© 2011 Paessler AG

Basic Sensor Settings	
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Virtual Machine Settings	
GUID	Shows the Globally Unique Identifier (GUID) of the virtual machine. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the virtual machine. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Operating System	Shows the operating system on the virtual machine. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Handling of "Powered off" VM	Choose how the sensor will react to a virtual machine that is powered off. Please choose between: • **Ignore "powered off" state (default)**: The sensor will not change to a down status if the virtual machine is powered off; it will report zero values instead. • **Alarm when VM is "powered off"**: The sensor will change to a down status if the virtual machine is powered off.
Compatibility	Define how the sensor will connect. Choose between: ▪ **Default Method**: Use the default method for connection. ▪ **Alternate Method (.NET required)**: Use an other method to connect. Choose this option if you experience connection problems. It requires .NET (version 1 or higher) to be installed on the system running the PRTG probe this sensor is created on.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.85 WBEM Custom Sensor

The WBEM Custom Sensor performs a custom query via Web-Based Enterprise Management (WBEM). It can show the total and channels received.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WBEM Custom Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Custom Query Specific	
Namespace	Enter the namespace for the query. Default value is **root/cimv2**.
WBEM Query (WQL)	Enter the WBEM Query that will be performed with every scanning interval. It has to be written in CQL/WQL.
Numeric Format	Define how the returned values will be handled as. Choose between: ▪ **Integer**: The query returns integer values. ▪ **Float**: The query returns float values.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

More

For more tips and tricks regarding WQL scripts, please see the Paessler Knowledge Base and search for **WQL**.

- http://www.paessler.com/knowledgebase

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

© 2011 Paessler AG

Others

For more general information about settings, please see Object Settings 111 section.

6.7.86 Windows Last Update Sensor

The Windows Last Update sensor reads the number of days since last Windows update from its parent device and returns the number of days. Use threshold triggers 797 to get notified in case this number breaches a certain value.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Enable Remote Registry Service

In order for this sensor to work, you need to enable the *Remote Registry* Windows service on the target machine. To do so, please log in to this machine and open the services manager (e.g. start *services.msc*). In the list of services, find the **Remote Registry** service and set its *Start Type* to *Automatic*.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Windows Last Update Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Timeout (sec.)	Define the timeout for the internal process. It will be killed if it has not returned a result after this time. Please enter an integer value.

© 2011 Paessler AG

Sensor Settings	
If Value Changes	Define what will be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change. • **Trigger 'change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.87 Windows Logged In Users Sensor

The Windows Logged In Users sensor queries the number of users logged in to a Windows installation on the parent device. It returns the total number. You can optionally filter for certain user names.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Windows Logged In Users Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
User Filter (optional)	To filter the value returned by certain user names, define them here. Enter a comma separated list of user names, or leave the field empty.
Processing of Users in "User Filter"	Define how the user names entered above will be used. Choose between: ▪ **Do not count users listed in "User Filter"**: Exclude the users entered above from counting and only count other uses. ▪ **Only count users listed in "User Filter"**: Ignore all other users and only count user names from the list entered above.
If Value Changes	Define what will be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change.

Sensor Settings	
	• **Trigger 'change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.88 Windows MSMQ Queue Length Sensor

The Windows MSMQ Queue Length sensor reads the number of messages in a Microsoft Message Queue of the parent device. It gives back the total number.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Windows MSMQ Queue Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Message Queue Name	Define the name of the message queue you want to check. Please enter a string.
Message Queue Type	Define the type of the message queue entered above. Choose between: ▪ **Private** ▪ **Public**
Min. Message Age	Optionally define the age in minutes. If set, messages younger than this will not be regarded. Please enter an integer value or leave the field empty.

© 2011 Paessler AG

Sensor Settings	
Timeout (sec.)	Define the timeout for the request. It will be killed if it has not returned a result after this time. Please enter an integer value.
If Value Changes	Define what will be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change. • **Trigger 'change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.
Results	Define what will be done with the result received. Choose between: • **Discard result**: Do not store the requested web page. • **Write result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the script to the "Logs (System)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see **More** 256 section below.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.89 Windows Print Queue Sensor

The Windows Print Queue sensor reads the print queue on its parent device and gives back the number of jobs in the print queue, if a print server is running on the parent device. Additionally, this sensor can change to a **Warning** status if there is a problem, such as out of paper, etc. *Note:* You can only check print servers running in the same domain than the one defined in the parent device's Windows credential settings.

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.

Required *.NET* version: 3.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Windows Print Queue Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Print Queue Name	Define the name of the print queue you want to check. Usually, the name is identical with the printer name shown on the target machine's desktop. Please enter a string.
Min. Print Job Age (sec.)	Optionally define the age in sedonds. If set, jobs younger than this will not be regarded. Please enter an integer value or leave the field empty.

Sensor Settings	
Min. Print Job Age (sec.)	Define if the sensor will change to a **Warning** status in case a printer reports a problem. Choose between: ▪ **No** ▪ **Yes**

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.90 WMI CPU Load Sensor

The WMI CPU Load sensor monitors the CPU load on a computer via Windows Management Instrumentation (WMI). It shows the CPU usage in percent.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI CPU Load Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Alternative Query	
Errors and invalid data	This is an extended help field only. PRTG's WMI sensors are equipped with the most efficient and accurate WMI queries. However, Microsoft has changed (and will continue to do that in the future) some WMI classes over the various Windows/ServicePack/patchlevel versions, resulting in errors like "class not valid" or "invalid data". Wherever possible PRTG features an alternative query that might work in your specific circumstances. When you keep getting errors for this sensor please try enabling the alternative query method below.
Alternative query	Choose the method PRTG uses to query via WMI. For compatibility reasons, an alternative query method can be enabled. We recommend using the default value. You can choose between: • **use default**: Use PRTG's standard method to query WMI. This is the best setting in most cases.

© 2011 Paessler AG

WMI Alternative Query	
	• **use alternative**: Use an alternative method to query WMI. If you keep getting errors, please try this setting.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.91 WMI Custom Sensor

The WMI Custom Sensor performs a custom query via Windows Management Instrumentation (WMI).

Note: Your Windows Management Instrumentation Query Language (WQL) query code must be stored in a file on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Custom Query Specific	
Channel Name	Enter a name for the channel in which the received data will be presented. The name will be displayed in graphs and tables. Please enter a string. You can change the name later in the sensor's channel settings 792.

WMI Custom Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

Custom Query Specific	
Namespace	Enter the namespace for the query.
WQL-File	Select a file that will be used for this sensor from the drop down menu. It will be executed with every scanning interval. The menu contains WQL scripts from the **\Custom Sensors\WMI WQL scripts** sub folder of your PRTG installation. Please store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node!
Placeholder <#PH1>	In your WQL script, you can use up to three placeholders that you can assign a value to using this field. Please enter a string for variable **<#PH1>** or leave the field empty.
Placeholder <#PH2>	In your WQL script, you can use up to three placeholders that you can assign a value to using this field. Please enter a string for variable **<#PH2>** or leave the field empty.
Placeholder <#PH3>	In your WQL script, you can use up to three placeholders that you can assign a value to using this field. Please enter a string for variable **<#PH3>** or leave the field empty.
If value changes	Define what shall be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change. • **Trigger 'On Change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.
Channel Name	Enter a name for the channel in which the received data will be presented. The name will be displayed in graphs and tables. Please enter a string.
Unit String	Enter a unit for the data that will be received by your script. This is for displaying purposes only. The unit will be displayed in graphs and tables. Please enter a string.
Multiplication	Define with which value the received values will be multiplied by. By default, this is set to **1** in order to not change the received values. Please enter an integer, a decimal value, or leave the field empty.
Division	Define with which value the received values will be divided by. By default, this is set to **1** in order to not change the received values. Please enter an integer, a decimal value, or leave the field empty.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

More

▪ Additional Sensor Types (Custom Sensors) 790

Paessler Knowledge Base: How and Where Does PRTG Store its Data?
▪ http://www.paessler.com/knowledgebase/en/topic/463

For more tips and tricks regarding WQL scripts, please see the Paessler Knowledge Base and search for **WQL**.
▪ http://www.paessler.com/knowledgebase

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

© 2011 Paessler AG

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.92 WMI Event Log Sensor

The WMI Event Log sensor monitors a specific Windows log file using Windows Management Instrumentation (WMI). It shows the number of new records (volume), the number of new records per second (speed), and it returns the last message in the sensor status.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one log file, multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Eventlog Monitor	
Log file	The Windows event log provides several different log files. A list specific to your system is shown. Please select one or more log files from the list by adding a check mark in front of the respective line. For each log one sensor will be created. The log file setting of a sensor cannot be changed later.

WMI Event Log Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

WMI Event Log Monitor	
Log file	Shows the Windows log file that this sensor will monitor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Filter Event Log Entries	
Filter by Source	Filter all received events for a certain event source. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • **Off**: Do not filter by event source. • **On**: Enable filtering by event source.
Match String (Event Source)	This field is only visible if filtering is enabled above. Enter a source from which the events are to come from. Only events from a source matching this string will be regarded, others ignored. You can also use the percent sign (*%*) as placeholder for any or no character (as known from the asterisk sign (***) in Windows search) in combination with a substring. For example, you can enter **%RAS%** for any event source containing the string **RAS**. Please enter a string.
Filter by ID	Filter all received events for a certain event ID. If enabled, only messages matching the defined value(s) will be considered by the sensor. Choose between: • **Off**: Do not filter by event ID. • **On**: Enable filtering by event ID.
Match Value (Event ID)	This field is only visible if filtering is enabled above. Enter one or more event IDs (comma separated) from which the events are to come from. Only events with an ID matching one of the values will be regarded. Please enter one integer value or more comma separated integer values.
Filter by Category	Filter all received events for a certain event category. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • **Off**: Do not filter by event category. • **On**: Enable filtering by event category.
Match String (Event Category)	This field is only visible if filtering is enabled above. Enter a category which the events are to have. Only events with a category matching this string will be regarded. You can also use the percent sign (*%*) as placeholder for any or no character (as known from the asterisk sign (***) in Windows search) in combination with a substring. For example, you can enter **%N%** for any event category containing the character **N**. Please enter a string.
Filter by Event User	Filter all received events for a certain event user. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • **Off**: Do not filter by event user. • **On**: Enable filtering by event user.

Filter Event Log Entries	
Match String (Event User)	This field is only visible if filtering is enabled above. Enter a user name which the event are to be assigned to. Only events with a user name matching this string will be regarded. You can also use the percent sign (*%*) as placeholder for any or no character (as known from the asterisk sign (*) in Windows search) in combination with a substring. For example, you can enter **A%** for any user name starting with the character **A**. Please enter a string.
Filter by Event Computer	Filter all received events for a certain event computer. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • **Off**: Do not filter by event computer. • **On**: Enable filtering by event computer.
Match String (Event Computer)	This field is only visible if filtering is enabled above. Enter a computer name which the events are to be assigned to. Only events with a computer name matching this string will be regarded. You can also use the percent sign (*%*) as placeholder for any or no character (as known from the asterisk sign (*) in Windows search) in combination with a substring. Please enter a string.
Filter by Event Message	Filter all received events for a certain event message. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • **Off**: Do not filter by event message. • **On**: Enable filtering by event message.
Match String (Event Message)	This field is only visible if filtering is enabled above. Enter a message which the event must contain. Only events with a message matching this string will be regarded. You can use the percent sign (*%*) as placeholder for any or no character (as known from the asterisk sign (*) in Windows search) in combination with a substring here. Please enter a string.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).

© 2011 Paessler AG

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.93 WMI Exchange Server 2003 Sensor

The WMI Exchange Server 2003 Sensor monitors a Microsoft Exchange Server 2003 using Windows Management Instrumentation (WMI). It can show information about the queue, delivery time, and latency.

For this sensor type, Windows credentials must be defined for the device you want to use the sensor on.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Exchangeserver 2003 Monitor	
WMI Selection	You see a list of data values the sensor can monitor on your Exchange server. Please select one from the list. You can only select one value at a time. The available options depend on your Exchange server configuration. You might be able to select aspects regarding: ▪ **Queue Number of Messages/Size** ▪ **SMTP Server Local/Remote/Categorizer Queue Length** ▪ **Mailbox** and **Public Send/Receive Queue Size** ▪ **Mailbox Average Delivery Time** ▪ **RPC Requests/Averaged Latency** With each sensor created you can monitor one of these aspects. If you want to monitor different aspects at the same time, please add this sensor multiple times. The easiest way to add multiple sensors is to use the **Run Auto-Discovery** 146 option in your Exchange server device's context menu 128.

WMI Exchange Server 2003 Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Exchangeserver 2003 Monitor	
WMI Selection	Shows the type of data that this sensor monitors on the Exchange server. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.94 WMI Exchange Server 2007 Sensor

The WMI Exchange Server 2007 sensor monitors a Microsoft Exchange Server 2007 using Windows Management Instrumentation (WMI). It can show information about the queue, delivery time, and latency.

In our tests, this sensor also works with Exchange Server 2010.

For this sensor type, Windows credentials must be defined for the device you want to use the sensor on.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Exchangeserver Monitor	
WMI Selection	You see a list of data values the sensor can monitor on your Exchange server. Please select one from the list. You can only select one value at a time. The available options depend on your Exchange server configuration. You might be able to select aspects regarding: ▪ **Messages Delivered/Sent/Submitted/Queued** and **Average Delivery Time** for **Mailbox** and **Public** ▪ **RPC Requests/Averaged Latency/Operations/Num. of Slow Packets** ▪ **Database (Information Store) Page Fault Stalls/Log Record Stalls** ▪ **Log Threads Waiting/Cache Size/Cache % Hit** ▪ **Store Interface RPC Latency** ▪ **Store Interface Requests Outstanding/Failed/Sent/Slow/Latency** ▪ **Store Interface ROP Requests Outstanding** With each sensor created you can monitor one of these aspects. If you want to monitor different aspects at the same time, please add this sensor multiple times. The easiest way to add multiple sensors is to use the **Run Auto-Discovery** 146 option in your Exchange server device's context menu 128.

WMI Exchange Server 2007 Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Exchangeserver Monitor	
WMI Selection	Shows the type of data that this sensor monitors on the Exchange server. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.95 WMI File Sensor

The WMI File monitors a file using Windows Management Instrumentation (WMI). It shows the file size and the last modified date.

For a general introduction to the technology behind WMI, please see Monitoring via WMI 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI File Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI File Monitor	
File name	Enter the name of the file that this sensor will check. Please enter a full local path. The file must exist on the computer your local or remote probe is running on; UNC paths are not allowed here. For example, when creating this sensor on a device under the local probe, the file be accessible on the local system.
If timestamp changes	Define what shall be done in case the timestamp of the file changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change. • **Trigger 'On Change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.96 WMI Free Disk Space (Single Disk) Sensor

The WMI Disk Space (Single Disk) sensor monitors the free disk space on one drive or one logical volume using Windows Management Instrumentation (WMI). It shows the space in percent and total. For each drive or logical volume, one sensor is used.

Note: This sensor is not supported on Windows XP and earlier.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

For devices with multiple volumes multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Volume Specific	
Volumes	From the list, select the volume(s) you want to monitor. The list shows all available volumes on the device. Please select one or more volume(s) by adding a check mark in front of the respective line.

WMI Free Disk Space (Single Disk) Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

WMI Volume Specific	
DeviceID	Shows the id of the volume that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Drive Type	Shows the type of the drive the sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Timeout (sec)	Enter a timeout in seconds for the WMI request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.97 WMI Free Disk Space (Multi Drive) Sensor

The WMI Free Disk Space (Multi Drive) sensor monitors the free disk space of one or multiple drive(s) using Windows Management Instrumentation (WMI). It shows the space in percent and total. One single sensor is used for all drives; the data is presented in different channels.

Note: This sensor is also supported on Windows XP and earlier.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Volume Specific	
Drive	From the drop down menu select the drive(s) you want to monitor. We recommend using the default value. You can choose **All** to monitor all available drives or you can choose one specific drive letter to monitor this single drive only. The data in the drop down menu may also contain drive letters that do not exist on your device. The drive setting cannot be changed once the sensor is created.

WMI Disk Space (Single Disk) Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Disk Free Configuration	
Drive	Shows the drive(s) that this sensor is monitoring; either **All** or a specific drive letter. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Set limits checked against ALL disks	
In this section you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor will enter a warning or down state; depending on the data provided by all drives that this sensor monitors. If you want to define limits for separate channels individually please use the limit settings in the sensor's **Channels** tab. *Note:* All limits defined here are valid additionally to the limits defined in the **Channels** tab!	
Percentage Limit Check	Enable or disable a limit check for the free space in percentage channels of all drives. By default percentage limits are enabled with lower warning and lower error limit. Choose between: • **Disable Percentage Limits**: Do not use the drives' data to control the sensor's status. • **Enable Percentage Limits**: Define limits. Additional fields appear below. The sensor will enter a warning or down state when free space limits are undercut or overrun.
Upper Error Limit	This field is only visible if percentage limit check is enabled above. Specify an upper limit in percent for an error state. If the free disk space of one of your drives overruns this percent value, the sensor will be set to down. Please enter an integer value or leave the field empty.
Upper Warning Limit	This field is only visible if percentage limit check is enabled above. Specify an upper limit in percent for a warning state. If the free disk space of one of your drives overruns this percent value, the sensor will be set to warning. Please enter an integer value or leave the field empty.
Lower Warning Limit	This field is only visible if percentage limit check is enabled above. Specify a lower limit in percent for a warning state. If the free disk space of one of your drives undercuts this percent value, the sensor will be set to warning. Please enter an integer value or leave the field empty.
Lower Error Limit	This field is only visible if percentage limit check is enabled above. Specify a lower limit in percent for an error state. If the free disk space of one of your drives undercuts this percent value, the sensor will be set to down. Please enter an integer value or leave the field empty.
Byte Limit Check	Enable or disable a limit check for the free bytes channels of all drives. Choose between: • **Disable Byte Limits**: Do not use the drives' data to control the sensor's status. • **Enable Byte Limits**: Define limits. Additional fields appear below. The sensor will enter a warning or down state when free space limits are undercut or overrun.

© 2011 Paessler AG

Set limits checked against ALL disks	
Upper Error Limit	This field is only visible if byte limit check is enabled above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor will be set to down. Please enter an integer value or leave the field empty. *Note:* The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings 792. The limits set here and in the channel settings are valid simultaneously!
Upper Warning Limit	This field is only visible if byte limit check is enabled above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor will be set to warning. Please enter an integer value or leave the field empty. *Note:* The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings 792. The limits set here and in the channel settings are valid simultaneously!
Lower Warning Limit	This field is only visible if byte limit check is enabled above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor will be set to warning. Please enter an integer value or leave the field empty. *Note:* The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings 792. The limits set here and in the channel settings are valid simultaneously!
Lower Error Limit	This field is only visible if byte limit check is enabled above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor will be set to down. Please enter an integer value or leave the field empty. *Note:* The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings 792. The limits set here and in the channel settings are valid simultaneously!

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.98 WMI IIS 6.0 SMTP Received Sensor

The WMI IIS 6.0 SMTP Receiver Sensor monitors Microsoft's Internet Information Services regarding the number of received emails for an IIS 6.0 SMTP service (Exchange 2003) using Windows Management Instrumentation (WMI). It shows the number of messages, the bytes, and the number of retries, per second for received messages.

Note: This service is not used by Exchange Server 2007 and higher. Exchange Server 2007 uses its own SMTP stack implemented in the Microsoft Exchange Transport service.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI IIS 6.0 SMTP Received Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.99 WMI IIS 6.0 SMTP Sent Sensor

The WMI IIS 6.0 SMTP Sent Sensor monitors Microsoft's Internet Information Services regarding the number of sent emails for an IIS 6.0 SMTP service (Exchange 2003) using Windows Management Instrumentation (WMI). It shows the number of messages, the bytes, and the number of retries, per second for sent messages.

Note: This service is not used by Exchange Server 2007 and higher. Exchange Server 2007 uses its own SMTP stack implemented in the Microsoft Exchange Transport service.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI IIS 6.0 SMTP Sent Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.100 WMI Memory Sensor

The WMI Memory sensor monitors available system memory systems using Windows Management Instrumentation (WMI).

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI Memory Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Alternative Query	
Errors and invalid data	This is an extended help field only. PRTG's WMI sensors are equipped with the most efficient and accurate WMI queries. However, Microsoft has changed (and will continue to do that in the future) some WMI classes over the various Windows/ServicePack/patchlevel versions, resulting in errors like "class not valid" or "invalid data". Wherever possible PRTG features an alternative query that might work in your specific circumstances. When you keep getting errors for this sensor please try enabling the alternative query method below.
Alternative query	Choose the method PRTG uses to query via WMI. For compatibility reasons, an alternative query method can be enabled. We recommend using the default value. You can choose between: • **use default**: Use PRTG's standard method to query WMI. This is the best setting in most cases.

© 2011 Paessler AG

WMI Alternative Query	
	• **use alternative**: Use an alternative method to query WMI. If you keep getting errors, please try this setting.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see **Sensor Channels Settings** 792 section.

© 2011 Paessler AG

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.101 WMI Microsoft SQL Server 2005 Sensor

The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL server via Windows Management Instrumentation (WMI). It can show the number of user connections, and the number of logins and logouts per second; the number of full scans, page splits, and table lock escalations, per second; the buffer cache hit ratio in percent, and the number of database pages and stolen pages; the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory, in KB; the number of lock requests and deadlocks, per second, and the average wait time; and the number of batch requests, SQL compilations, and SQL re-compilations, per second. The channels actually available for a sensor depend on which performance counters you choose during setup.

Note: This sensor can only be added to a device (computer) running a Microsoft SQL database.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI Microsoft SQL Server Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

SQL Server Settings	
MS SQL Server Instance	A list of all Microsoft SQL database instances running on the parent device is shown. Select a database by adding a check mark in front of its name. For each combination of database and counter set one sensor will be created. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SQL Counter Specific Settings	
SQL Performance Counters	Define which kind of counters the sensor will monitor. For each combination of database and counter one sensor will be created. Choose between: ▪ **General Statistics**: Read general performance counters. This will show the number of user connections, and the number of logins and logouts per second. ▪ **Access Methods**: Read access method counters. This will show the number of full scans, page splits, and table lock escalations, per second. ▪ **Buffer Manager**: Read buffer manager counters. This will show the buffer cache hit ratio in percent, and the number of database pages and stolen pages. ▪ **Memory Manager**: Read memory manager counters. This will show the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory, in KB. ▪ **Locks**: Read locks counters. This will show the number of lock requests and deadlocks, per second, and the average wait time. ▪ **SQL Statistics**: Read SQL statistics. This will show the number of batch requests, SQL compilations, and SQL re-compilations, per second. Depending on your selection, a sensor with the specified channels will be created. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew. You can add this sensor several times, with other counters each.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.102 WMI Microsoft SQL Server 2008 Sensor

The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL server via Windows Management Instrumentation (WMI). It can show the number of user connections, and the number of logins and logouts per second; the number of full scans, page splits, and table lock escalations, per second; the buffer cache hit ratio in percent, and the number of database pages and stolen pages; the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory, in KB; the number of lock requests and deadlocks, per second, and the average wait time; and the number of batch requests, SQL compilations, and SQL re-compilations, per second. The channels actually available for a sensor depend on which performance counters you choose during setup.

Note: This sensor can only be added to a device (computer) running a Microsoft SQL database.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI Microsoft SQL Server Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SQL Server Settings	
MS SQL Server Instance	A list of all Microsoft SQL database instances running on the parent device is shown. Select a database by adding a check mark in front of its name. For each combination of database and counter set one sensor will be created. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SQL Counter Specific Settings	
SQL Performance Counters	Define which kind of counters the sensor will monitor. For each combination of database and counter one sensor will be created. Choose between: ▪ **General Statistics**: Read general performance counters. This will show the number of user connections, and the number of logins and logouts per second. ▪ **Access Methods**: Read access method counters. This will show the number of full scans, page splits, and table lock escalations, per second. ▪ **Buffer Manager**: Read buffer manager counters. This will show the buffer cache hit ratio in percent, and the number of database pages and stolen pages. ▪ **Memory Manager**: Read memory manager counters. This will show the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory, in KB. ▪ **Locks**: Read locks counters. This will show the number of lock requests and deadlocks, per second, and the average wait time. ▪ **SQL Statistics**: Read SQL statistics. This will show the number of batch requests, SQL compilations, and SQL re-compilations, per second. Depending on your selection, a sensor with the specified channels will be created. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew. You can add this sensor several times, with other counters each.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.103 WMI Network Card Sensor

The WMI Network Card sensor monitors bandwidth usage and traffic of a network interface using Windows Management Instrumentation (WMI).

For a general introduction to the technology behind WMI, please see Monitoring via WMI 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

For devices with multiple network cards multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Specify network interface	Select the network card(s) you want to add a sensor for. A list of network cards is shown; containing all cards which your device provides. Select one or more cards by adding a check mark in front of a card's name.

WMI Network Card Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Selected Interface	Shows the name of the network card that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

© 2011 Paessler AG

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.104 WMI Pagefile Sensor

The WMI Pagefile sensor monitors the Windows pagefile usage via Windows Management Instrumentation (WMI). It shows the usage in percent. *Note:* This sensor does *not* work with Windows 2000, as the respective WMI class does not exist on this operating system!

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI Pagefile Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.105 WMI Process Sensor

The WMI Process sensor monitors a Windows process using Windows Management Instrumentation (WMI). It shows the absolute working set and commit size, processor time in percent, and the number of threads and handles.

For this sensor type, Windows credentials must be defined for the device you want to use the sensor on.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI Process Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Process Monitor	
Executable	Enter the name of the process that will be monitored. Please enter the name of an executable file without the *.exe* extension. The sensor will be set to an error state if the process is not active on the device.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.

© 2011 Paessler AG

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.106 WMI Service Sensor

The WMI Service sensor monitors a Windows service using Windows Management Instrumentation (WMI). It shows the total time the service runs.

For this sensor type, Windows credentials must be defined for the device you want to use the sensor on.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one service multiple sensors are created at once in the **Add Sensor** dialog.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Service Monitor	
Service	You see a list of all services available on the device, including the ones that are not running. Name and description are provided in the language of the device's Windows installation. Please choose one or more services by adding a check mark in front of the respective line. For each service one sensor will be created. Later on, a sensor's status will be set to down if the service is not running.

WMI Service Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.

Basic Sensor Settings	
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Service Monitor	
Service	Shows the Windows service this sensor will monitor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows the description for the service. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Start/Restart Service	Select whether the service will be started if it is stopped or passed. Choose between: • **Start/Restart service (default)**: PRTG will try to start the service if it is not running when scanning the device. • **Do nothing**: PRTG will not start any service on the device automatically.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

© 2011 Paessler AG

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.
Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.107 WMI Share Sensor

The WMI Share sensor monitors a shared resource on a Windows system using Windows Management Instrumentation (WMI). It shows the availability; you can trigger a sensor down state for different share status messages.

For this sensor type, Windows credentials must be defined for the device you want to use the sensor on.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one share multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Shared Recource	
Share	You see a list of all shares available on the device with name, type and description. Please choose one or more shares by adding a check mark in front of the respective line. For each share one sensor will be created with the settings below. *Note:* In order to provide any shares, the "Server" Windows service must be running on the target computer. If it is not, there are no shares and you will see a **No Share available** message here.

WMI Share Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.

© 2011 Paessler AG

Basic Sensor Settings	
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Shared Recource	
Shared Recource	Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Type	Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
TypeID	Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Trigger Errorstate on following conditions	
Select under which conditions the sensor will change to a down status from the list below. As long as the share returns OK, the sensor status will be ok. Choose a down condition by adding a check mark symbol in front of the according line. Please choose none, one, or several from the following conditions.	
Error	Set sensor to down status if the share returns an error status. A share in this status is not operational.
Degraded	Set sensor to down status if the share returns a degraded status. A share in this status is still operational.
Unknown	Set sensor to down status if the share returns an unknown status.
Pred Fail	Set sensor to down status if the share returns a "predicted fail" status. This indicates that an element is functioning properly but is predicting a failure (for example, a SMART-enabled hard drive). A share in this status is still operational.
Starting	Set sensor to down status if the share returns a starting status. A share in this status is not operational.
Stopping	Set sensor to down status if the share returns a stopping status. A share in this status is not operational.

Trigger Errorstate on following conditions	
Service	Set sensor to down status if the share returns a service status. This can apply during disk mirror-resilvering, reloading a user permissions list, or other administrative work on the monitored device. Not all such work is online, but the managed element is neither OK nor in one of the other states. A share in this status is not operational.
Stressed	Set sensor to down status if the share returns a stressed status.
Nonrecover	Set sensor to down status if the share returns a "non recover" status.
NoContact	Set sensor to down status if the share returns a "no contact" status.
LostComm	Set sensor to down status if the share returns "lost communication" status.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.108 WMI Terminal Services (Windows 2008) Sensor

The WMI Terminal Services sensor monitors the number of sessions on a Windows Terminal Services server using Windows Management Instrumentation (WMI). It shows the number of active and total sessions. Active sessions are sessions with a currently logged in user; inactive sessions (included in total) can be sessions with a disconnected user that has not logged out, or system services using a session.

Note: Depending on the OS that will be monitored, please select either the sensor for Windows XP/Vista/2003 or the one for Windows 2008.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI Terminal Services Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.109 WMI Terminal Services (Windows XP/Vista/2003) Sensor

The WMI Terminal Services sensor monitors the number of sessions on a Windows Terminal Services server using Windows Management Instrumentation (WMI). It shows the number of active and total sessions. Active sessions are sessions with a currently logged in user; inactive sessions (included in total) can be sessions with a disconnected user that has not logged out, or system services using a session.

Note: Depending on the OS that will be monitored, please select either the sensor for Windows XP/Vista/2003 or the one for Windows 2008.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI Terminal Services Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

© 2011 Paessler AG

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.110 WMI Uptime Sensor

The WMI Uptime sensor monitors uptime of a Windows system using Windows Management Instrumentation (WMI). It shows the uptime of system.

For a general introduction to the technology behind WMI, please see **Monitoring via WMI** 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI Uptime Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).

© 2011 Paessler AG

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.7.111 WMI Vital System Data Sensor

The WMI Vital System Data sensor monitors vital system parameters (CPU, system, memory, disk, network, server, and CLR memory) using Windows Management Instrumentation (WMI).

For this sensor type, Windows credentials must be defined for the device you want to use the sensor on.

For a general introduction to the technology behind WMI, please see Monitoring via WMI 938 section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Vital System Data Readings Accessible Using WMI	
WMI Vital System Data	You see a list of vital system data values. Please select one from the list. You can only select one value at a time. To add more than one value, please add this sensor several times. *Note:* Some of the shown options may not work on your target device. This depends on its Windows version and configuration. There are many different system parameters available. Choose between: ▪ **CPU: Percent Processor Time** ▪ **CPU: Processor Queue Length** ▪ **CPU: Processor Percent Privileged Time** ▪ **CPU: Processor Percent User Time** ▪ **System: Thread Context Switches/sec** ▪ **Memory: Free Physical Memory** ▪ **Memory: Total Visible Memory** ▪ **Memory: Pages/sec** ▪ **Memory: Page Faults/sec** ▪ **Memory: Page Reads/sec** ▪ **Memory: Page Writes/sec** ▪ **Memory: Percent Pagefile Usage** ▪ **Memory: Pool Nonpaged Bytes** ▪ **Memory: Pool Paged Bytes** ▪ **Memory: Cache Bytes** ▪ **Memory: Committed Bytes** ▪ **Disk: Percent Disk Time (Windows 2000/XP/Server2003 only)** ▪ **Disk: Current Disk Queue Length** ▪ **Disk: Bytes/sec (Windows 2000/XP/Server2003 only)** ▪ **Disk: Reads/sec (Windows 2000/XP/Server2003 only)** ▪ **Disk: Writes/sec (Windows 2000/XP/Server2003 only)** ▪ **Network: Bytes Total/sec** ▪ **Network: Bytes Received/sec** ▪ **Network: Bytes Sent/sec**

© 2011 Paessler AG

Vital System Data Readings Accessible Using WMI	
	▪ **Network: Packets Outbound Errors** ▪ **Server: Bytes Total/sec** ▪ **Server: Bytes Received/sec** ▪ **Server: Bytes Sent/sec** ▪ **CLR Memory: % Time in GC** ▪ **CLR Memory: # Bytes in all Heaps** ▪ **CLR Exceptions: # of Excepts Thrown / sec**

WMI Service Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Vital System Data Readings Accessible Using WMI	
WMI Vital System Data	Shows the type of system data that this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel.

Sensor Display	
	▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.112 WMI Windows Version Sensor

The WMI Windows Version sensor reads the Windows version of the parent device via Windows Management Instrumentation (WMI). It returns the version number (in a channel) as well as the according version name (in the sensor message).

This sensor requires the *Microsoft .NET Framework* to be installed on the computer running the PRTG probe: Either on the local system (on every node, if in a cluster), or on the system running the remote probe 987. If the framework is missing, you cannot create this sensor.
Required *.NET* version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

WMI Windows Version Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
If Value Changes	Define what will be done in case the value of this sensor changes. You can choose between: • **Ignore changes (default)**: No action will be taken on change. • **Trigger 'change' notification**: The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to trigger a notification 797 whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the **Sensor Channels Settings** 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the **Root** 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

© 2011 Paessler AG

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ **Bandwidth** ▪ **Memory** ▪ **Disk** ▪ **File** ▪ **Custom** *Note:* Custom channel types can be set on sensor level only.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

© 2011 Paessler AG

6.7.113 Xen Virtual Machine Sensor

The XEN Virtual Machine sensor monitors a virtual machine on a XEN server via Hypertext Transfer Protocol (HTTP) and Remote Procedure Call (RPC). It shows CPU usage and free memory in percent.
Note: The parent device must be a Citrix XenServer.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device manually 165. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Note: PRTG requests a full list of all virtual machines configured on the device. Therefore, it may take a few seconds before the dialog is loaded.

If you select more than one virtual machine multiple sensors are created at once in the **Add Sensor** dialog. The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Virtual Machine Settings	
Virtual Machine	You see a list of all virtual machines (VMs) available on the host server on this device. All VMs are listed with name and description. Please choose one or more machines by adding a check mark in front of the respective line. For each VM one sensor will be created.

XEN Virtual Machine Sensor Settings

On the sensor's detail page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Tags are automatically inherited 84.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

© 2011 Paessler AG

Virtual Machine Settings	
UUID	Shows the Universally Unique Identifier (UUID) of the virtual machine. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the virtual machine. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows the description information for the virtual machine. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.
Chart Type	Define how different channels will be shown for this sensor. ▪ **Show channels independently (default)**: Show an own graph for each channel. ▪ **Stack channels on top of each other**: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. *Note:* This option cannot be used in combination with manual *Vertical Axis Scaling* (available in the Sensor Channels Settings 792 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the Root 166 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 871.

Schedules and Dependencies	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings 862. *Note:* Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ **Use parent**: Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency. ▪ **Select object**: Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below. ▪ **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency. *Note:* Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector 120 to choose an object on which the current sensor will be dependent on.

© 2011 Paessler AG

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists and in the sensor tree. Exception: If a child object is visible to the user, the object is visible in the sensor tree, though not accessible. • **Read**: Users in this group can see the object and review its monitoring results. • **Write**: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. • **Full**: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

Channels

Click on the **Channels** tab to change display settings. For detailed information, please see Sensor Channels Settings 792 section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see Sensor Notifications Settings 797 section.

Others

For more general information about settings, please see Object Settings 111 section.

6.8 Additional Sensor Types (Custom Sensors)

Users can create and use their own, self-written custom sensors in PRTG Network Monitor to go far beyond PRTG's standard sensor set. You can create your own sensors using Windows Management Instrumentation Query Language (WQL), visual basic scripting, PowerShell, batch scripting, and by compiling an EXE or DLL file (using any Windows software development tool).

Basics

For a general introduction, please see the sections about EXE/Script sensors and the API documentation which contains details about the necessary return format for those sensors. WMI Custom sensors allow executing WQL requests.

- EXE/Script Sensor 251
- EXE/Script Advanced Sensor 258
- Application Programming Interface (API) Definition 979
- WMI Custom Sensor 680

Custom Sensors Included in PRTG

After installing PRTG Network Monitor you will already find a selection of custom EXE/Script and WMI WQL sensors in the installation path on your disk. Many of these are sample projects that you can edit and improve for your needs.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\EXE

- Demo Batchfile - Returns 200.bat
- Demo Batchfile - Set sensorstate to warning.bat
- Demo Cmd - Returns 200.cmd
- Demo Dll - Returns a random integer.dll
- Demo EXE - Returns a random integer.exe
- Demo EXE - Returns number of files in folder (parameter).exe
- Demo EXE - Returns user of process.exe
- Demo Powershell Script - Available MB via WMI.ps1
- Demo Powershell Script - Check EXE Sensor Parameters.ps1
- Demo Powershell Script - InterruptsPerSec via WMI.ps1
- Demo Powershell Script - Returns a fixed integer value.ps1
- Demo Powershell Script - Returns a random integer value.ps1
- Demo Powershell Script - Returns Random Integer and Warnings.ps1
- Demo VBScript - Check EXE Sensor Parameters.vbs
- Demo VBScript - InterruptsPerSec via WMI.vbs
- Demo VBScript - Multiplies two integers(2 parameters).vbs
- Demo VBScript - Returns a fixed float value.vbs
- Demo VBScript - Returns a fixed integer value.vbs
- Demo VBScript - Returns a random value.vbs
- Demo VBScript - Returns number of svchost processes.vbs
- Demo VBScript - Returns user of process.vbs
- Demo VBScript - Returns warning depending on number of svchost processes.vbs
- Demo VBScript - UTCTime via WMI.vbs
- Load_Test_CPU_10_Mio_Primes.exe
- Load_Test_CPU_1_Mio_Primes.exe

© 2011 Paessler AG

- Load_Test_Disk_Write_Read_10000_files.exe
- Load_Test_Disk_Write_Read_1000_files.exe
- Load_Test_Memory_Allocate_And_Free_400MB.exe

To create a new sensor based on one of these files, create a new EXE/Script Sensor 251 and choose the respective file from the drop down list.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\EXEXML

- Demo Batchfile - Returns static values in four channels.bat

To create a new sensor based on one of these files, create a new EXE/Script Advanced Sensor 258 and choose the respective file from the drop down list.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\WMI WQL scripts

- Demo WQL Script - Get Win32LogicalDiscFreeMB.wql
- Demo WQL Script - Get Win32OsBuildnumber.wql
- Demo WQL Script - Get Win32PercentProcessorIdleTime.wql
- Demo WQL Script - Get Win32PercentProcessorTime.wql

To create a new sensor based on one of these files, create a new WMI Custom Sensor 680 and choose the respective file from the drop down list.

Downloading Pre-Build Custom Sensors

A good resource is the PRTG Add-Ons website on the open source platform *Google Code*. There are also additional tools available.

Open Source Add-Ons for PRTG Network Monitor V8 and later
- http://code.google.com/p/prtg-addons/

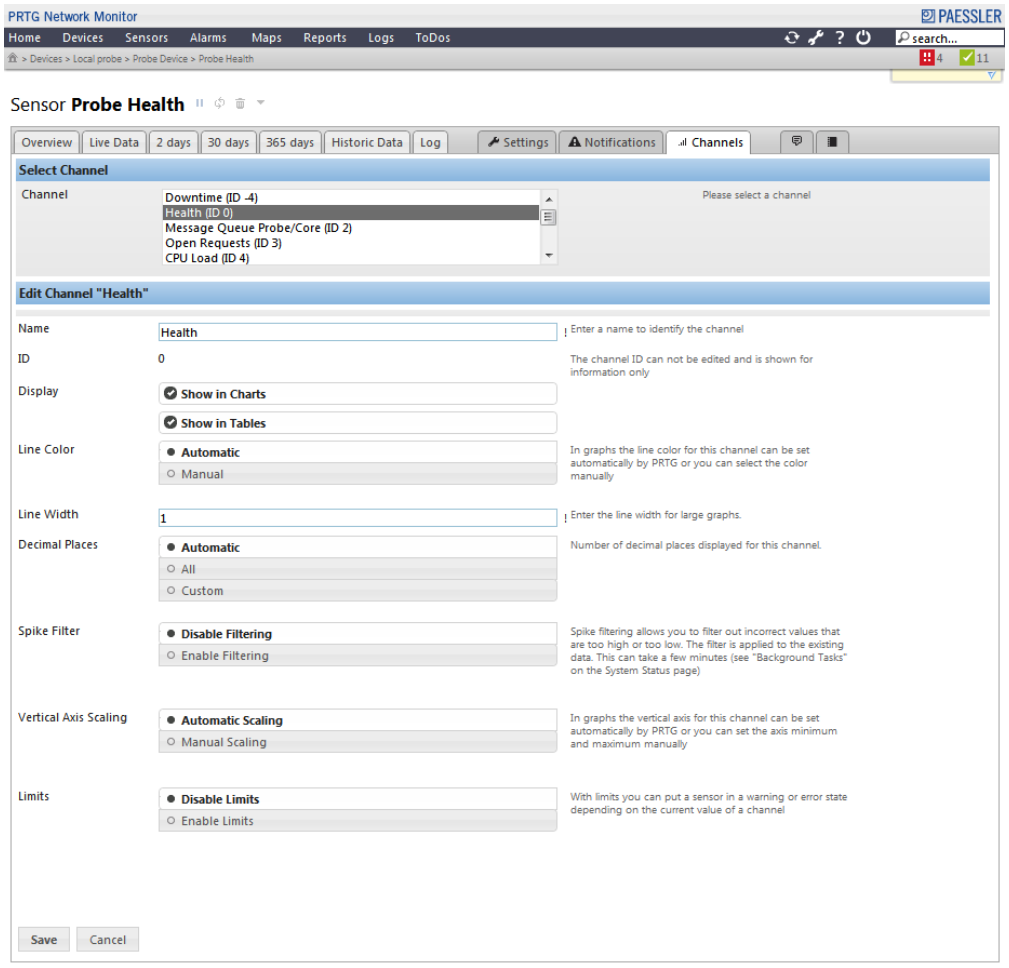
More

For the other sensor types that work out-of-the-box, please see List of Available Sensor Types 203.

6.9 Sensor Channels Settings

A sensor has one or more channels in which it handles the actual monitoring data. In the channel settings you can define how the data from the sensor's different channels shall be displayed in graphs and tables. Additionally, the channel data can affect the sensor's status. Use the limit settings to achieve this.

On the sensor's detail page, click on the **Channels** tab to change channel settings. The available options are the same for all sensors.


PRTG Network Monitor
PAESSLER
Home Devices Sensors Alarms Maps Reports Logs ToDos
search...
> Devices > Local probe > Probe Device > Probe Health
Sensor Probe Health
Overview Live Data 2 days 30 days 365 days Historic Data Log Settings Notifications Channels
Select Channel
Channel
Downtime (ID -4)
Health (ID 0)
Message Queue Probe/Core (ID 2)
Open Requests (ID 3)
CPU Load (ID 4)
Please select a channel
Edit Channel "Health"
Name
Health
Enter a name to identify the channel
ID
0
The channel ID can not be edited and is shown for information only
Display
Show in Charts
Show in Tables
Line Color
Automatic
Manual
In graphs the line color for this channel can be set automatically by PRTG or you can select the color manually
Line Width
1
Enter the line width for large graphs.
Decimal Places
Automatic
All
Custom
Number of decimal places displayed for this channel.
Spike Filter
Disable Filtering
Enable Filtering
Spike filtering allows you to filter out incorrect values that are too high or too low. The filter is applied to the existing data. This can take a few minutes (see "Background Tasks" on the System Status page)
Vertical Axis Scaling
Automatic Scaling
Manual Scaling
In graphs the vertical axis for this channel can be set automatically by PRTG or you can set the axis minimum and maximum manually
Limits
Disable Limits
Enable Limits
With limits you can put a sensor in a warning or error state depending on the current value of a channel
Save
Cancel

Channel Settings for Probe Health Sensor

© 2011 Paessler AG

Available Channel Settings

Select Channel	
Channel	From the list, select the channel you want to change settings for. All settings below belong to the channel selected here. The content of the list depends on what channels are available for this sensor. The **Downtime** channel is different from other channels and not all setting options are available for it. *Note:* If you change the channel here then all unsaved settings below will be lost.

Edit Channel "[Name]"	
Name	Enter a meaningful name to identify the channel. The name will be shown in graphs and tables. You can automatically add the sensor's ID to the name by using the placeholder **[#id]**.
ID	The ID of the channel cannot be changed; it is used for unique definition. For example, you need the ID when using Sensor Factory 497 sensors.
Display	Choose where the channel shall be displayed. You can choose from • **Show in Charts** • **Show in Tables** To change this setting, remove or add the check mark symbol in front of it.
Line Color	Define in what color the channel shall be displayed in graphs. You can choose between • **Automatic** • **Manual** When you set this option to manual color definition please enter a color below.
Color (#rrggbb)	This option is only available if **Manual** is selected in the **Line Color** setting above. Please either enter a color in hexadecimal RGB notation (as in HTML/CSS), or choose a color from the visual color selector. The field containing the hexadecimal color value will change to the resulting color immediately in both cases.
Line Width	Define in what color the channel shall be displayed in graphs. Enter an integer value in pixels. Although the line width is not limited, we recommend using values between 1 and 7 only in order to achieve optimal results.
Decimal Places	Define how many decimal places of the channel's data shall be displayed in graphs and tables. You can choose between • **Automatic**: Let PRTG choose how many decimal places will be used for optimal viewing results. • **All**: Force display of all available decimal places.

© 2011 Paessler AG

Edit Channel "[Name]"	
	• **Custom**: Manually define the number of decimal places. If you choose this option, an additional field will appear. Please enter an integer value there.
Spike Filter	A spike filter can be used to correct obviously faulty monitoring data. Sometimes, sensors report enormously high or far too low values; due to an error in data transmission, or due to incompatibilities of the physical device you are monitoring. This can make graphs unreadable. A spike filter can compensate for these flaws. When enabled values above and below a certain limit are disregarded in the monitoring data for graphs and tables. *Note:* The monitoring data itself will not be changed (but only the presentation of the data) and this setting is valid for all data of this channel (also the historic data). You can choose between • **Disable Filtering**: Display all data as it is; do not filter out spikes. • **Enable Filtering**: Enable a filter to remove spike values. Additional fields appear below. *Note:* The spike filter option is not available for the channel **Downtime**.
Spike Filter Max. Value [unit]	This field is only visible if spike filter is enabled above. Specify the maximum value allowed in the channel's data. All values above this value will be disregarded in graphs and tables. Please enter an integer value or leave the field empty.
Spike Filter Min. Value [unit]	This field is only visible if spike filter is enabled above. Specify the minimum value allowed in the channel's data. All values below this value will be disregarded in graphs and tables. Please enter an integer value or leave the field empty.
Vertical Axis Scaling	Define how the vertical axis for the channel is displayed in graphs. You can choose between • **Automatic Scaling**: Let PRTG decide on the optimum scaling; usually ranging from the minimum to the maximum value. PRTG will use one single scale for each unit label only. • **Manual Scaling**: Define the scaling manually. Additional fields appear below. Defining manual axis scaling can make low values better visible in your graph; but it may result in a chart with multiple vertical axis for the same unit label. *Note:* Settings for this option are ignored if *Chart Type* **Stack channels on top of each other** is enabled in the sensor's **Settings** tab.
Vertical Axis Maximum [unit]	This field is only visible if vertical axis scaling is enabled above. Specify the maximum value that shall be used on the vertical axis for the channel. Enter an integer value.
Vertical Axis Minimum [unit]	This field is only visible if vertical axis scaling is enabled above. Specify the minimum value that shall be used on the vertical axis for the channel. Enter an integer value.

© 2011 Paessler AG

Edit Channel "[Name]"	
Limits	The channel can affect the status of the sensor it is part of. By entering limits, you can define when the sensor shall enter a warning or down state; depending on the channel's data. Using this function, you can e.g. set a traffic sensor (which is usually never in a down state) to error when certain limits that you consider critical are reached. You can choose between • **Disable Limits**: Do not use the channel's data to control the sensor's status. • **Enable Limits**: Define limits. Additional fields appear below. The sensor belonging to the channel will enter a warning or down state when limits are undercut or overrun. *Note:* The limits option is not available for the channel "Downtime".
Upper Error Limit [unit]	This field is only visible if limits are enabled above. Specify an upper limit for an error state. If the channel's values overrun this value, the sensor will be set to down. Please enter an integer value or leave the field empty.
Upper Warning Limit [unit]	This field is only visible if limits are enabled above. Specify an upper limit for a warning state. If the channel's values overrun this value, the sensor will be set to warning. Please enter an integer value or leave the field empty.
Lower Warning Limit [unit]	This field is only visible if limits are enabled above. Specify a lower limit for a warning state. If the channel's values undercut this value, the sensor will be set to warning. Please enter an integer value or leave the field empty.
Lower Error Limit [unit]	This field is only visible if limits are enabled above. Specify a lower limit for an error state. If the channel's values undercut this value, the sensor will be set to down. Please enter an integer value or leave the field empty.
Error Limit Message	This field is only visible if limits are enabled above. Enter an additional message. It will be added to the sensor's message when entering a down status. Please enter a string or leave the field empty.
Warning Limit Message	This field is only visible if limits are enabled above. Enter an additional message. It will be added to the sensor's message when entering a warning status. Please enter a string or leave the field empty.

Click on **Save** to store your settings before you select another channel in the **Select Channel** section!

Sensor Settings Overview

For information about sensor settings, please see the following sections:

- Sensor Settings 202
- List of Available Sensor Types 203

© 2011 Paessler AG

6.10 Sensor Notifications Settings

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to you needs. Although it's the sensors that provoke a trigger, you can set notification triggers higher in the hierarchy (for example for groups or devices) and define triggers for multiple sensors by using the inheritance mechanism 82.

Note

This section describes one of three steps to set up the notification system in PRTG. A complete notification setup involves:

1. Defining notification delivery settings
2. Setting up notifications
3. Adding notification triggers to sensors

For more information please see **Notifications** 826 section.

Available Notification Triggers Settings

On an object's detail page, click on the **Notifications** tab to change sensor notification triggers. The available options are the same for all objects. When defining triggers for probes, groups, or devices they can be inherited down to sensor level.

Triggers that can be inherited from parent object(s)	
You see a list of all notification triggers that are defined higher in the hierarchy. The list is empty when there are no triggers defined in groups or devices above the current object. You can see the type and condition of the triggers, and the notifications that are executed once this trigger is provoked (for the transitions **On**, **Off**, **Escalation**).	
Trigger Inheritance	Define whether the triggers shown above will be handed on to the current object. Choose between: • **Inherit trigger(s) from parent object(s)**: Use the triggers shown above. • **Only use triggers defined for this object**: Do not use the triggers shown above; use only the triggers for this single object defined below. This setting is valid for all triggers shown above. It is not possible to only select some of them.

You can set up one or more of the following triggers, each with different setting options:

- State Triggers 798
- Speed Triggers 799
- Volume Triggers 800
- Threshold Triggers 801
- Change Triggers 802

State Triggers

Define triggers that are prompted when a sensor changes its current status. This is the most common reason to send out notifications. Click on the **Add State trigger** button to add a new trigger. Then define settings as described below. Every trigger will cause one or more notification(s) to be executed.

State Trigger(s)	
Condition	Select the condition that will trigger the notification. The trigger will be prompted when a sensor enters or leaves the selected status. Choose from the drop down menu: • **Down**: The trigger will be prompted if a sensor changes to a down status. • **Warning**: The trigger will be prompted if a sensor changes to a warning status. • **Unusual**: The trigger will be prompted if a sensor changes to an unusual status.
Latency (sec.)	Define how many seconds will be waited before an **On Notification** is triggered. This can avoid false alarms in case a sensor "flickers" and goes to a down status for just a few seconds. If the selected **Condition** (the sensor status) persists after the defined time span, the notification will be triggered. Please enter an integer value in seconds.
On Notification	Select a notification that will be triggered if the **Condition** (the sensor status) selected is true *and* the **Latency** time defined has passed. Choose a notification from the drop down menu. The menu shows all notifications defined in the notifications 825 setup. You can also choose **None** in order to only use other conditions for this trigger.
Off Notification	Select a notification that will be triggered if the **Condition** (the sensor status) selected is not true any more because the sensor's status changes again. **Latency** is not valid for this setting; an **Off Notification** will be sent as soon as the status changes.You can also choose **None** in order to only use other conditions for this trigger.
Esc. Latency (sec.)	Define an **Escalation Latency** in seconds. An escalation notification will be triggered if this number of seconds has passed since the sensor status has entered the defined condition. Using the escalation option, you can send additional notifications in case a problem persists for a longer time. Please enter an integer value in seconds.
Esc. Notification	Select a notification that will be triggered as **Escalation Notification** if the **Condition** (the sensor status) selected is still true *and* the **Esc. Latency** time defined has passed. You can use this option to trigger an additional notification after a certain time. For example, you can send notifications with an extended recipient list if a problem persists for a longer time. You can also choose **None** in order to only use other conditions for this trigger.

© 2011 Paessler AG

State Trigger(s)	
Repeat Every (min.)	Define a continuous repeat for an escalation notification. The escalation notification defined will be resent every x minutes. The repeat option is available for the escalation notification only. Please enter an integer value in minutes. You can also enter **0** in order to not use a repeat.
Delete	Click on the **Delete** button next to an existing notification trigger to delete it. *Note:* It will be deleted immediately and there is no warning message.

Click on the **Save** button at the end of the page to store your settings. You can then add another trigger.

Speed Triggers

Define triggers that will be prompted when a traffic sensor reaches a certain bandwidth limit for a specified time. Click on the **Add Speed trigger** button to add a new trigger. Then define settings as described below. Every trigger will cause one or more notification(s) to be executed.

Speed Trigger(s)	
Channel	Select the channel that will be regarded for this trigger from the drop down menu. Select **Primary** to use the sensor's primary channel (this can be defined in the sensor's settings 202) or choose a specific channel name from the list (there are different channels for every sensor type). All following settings for this trigger will be based on the chosen channel.
Condition	Select the condition that will trigger the notification. Choose from the drop down menu: • **Above**: The trigger will be prompted if the value of the selected channel overruns a defined value. • **Below**: The trigger will be prompted if the value of the selected channel undercuts a defined value. • **Equal**: The trigger will be prompted if the value of the selected channel is the same as a defined value. • **Not Equal**: The trigger will be prompted if the value of the selected channel is different than a defined value.
Value	Define the value the channel's data will be compared with. Please enter an integer value.
Scale	Select the unit in which you entered the value above. Choose from the drop down menu. The available values depend on the sensor you set this trigger for. **Scale** and **Time** together define the unit for the given value. If the channel's data is shown in a different unit PRTG will automatically convert values internally.
Time	Select the time for the scale (so you create a scale per time designation). Choose from the drop down menu: • **second** • **minute** • **hour**

Speed Trigger(s)	
	• **day** **Scale** and **Time** together define the unit for the given value. If the channel's data is shown in a different unit PRTG will automatically convert values internally.
Latency (sec.)	Define how many seconds will be waited before an **On Notification** is triggered. This can avoid false alarms in case a channel reaches a limit for just a few moments. If the combined channel condition (channel, condition, value, scale per time) persists after the defined time span, the notification will be triggered. Please enter an integer value in seconds.
On Notification	Select a notification that will be triggered if the combined channel condition (channel, condition, value, scale per time) is true *and* the **Latency** time defined has passed. Choose a notification from the drop down menu. The menu shows all notifications defined in the notifications 825 setup. You can also choose **None** in order to only use other conditions for this trigger.
Off Notification	Select a notification that will be triggered if the combined channel condition (channel, condition, value, scale per time) is not true any more because the channel's value changes again. **Latency** is not valid for this setting; an **Off Notification** will be sent as soon as the defined condition is not valid any more.You can also choose **None** in order to only use other conditions for this trigger.
Delete	Click on the **Delete** button next to an existing notification trigger to delete it. *Note:* It will be deleted immediately and there is no warning message.

No escalation notification and no repeat are available for this trigger type. Click on the **Save** button at the end of the page to store your settings. You can then add another trigger.

Volume Triggers

Define triggers that will be be prompted when a traffic sensor reaches a certain volume limit in a specified time. Click on the **Add Volume trigger** button to add a new trigger. Then define settings as described below. Every trigger will cause one notification to be executed.

Volume Trigger(s)	
Channel	Select the channel that will be regarded for this trigger from the drop down menu. Select **Primary** to use the sensor's primary channel (this can be defined in the sensor's settings 202) or choose a specific channel name from the list (there are different channels for every sensor type; a set of general channels is shown when adding triggers on group or device level). All following settings for this trigger will be based on the chosen channel.
Value	Define the value the channel's data will be compared with. If the channel's data overruns this value, a notification will be triggered. Please enter an integer value.

© 2011 Paessler AG

Volume Trigger(s)	
Scale	Select the unit in which you entered the value above. Choose from the drop down menu. The available values depend on the sensor you set this trigger for. **Scale** and **Period** together define the unit for the given value. If the channel's data is provided in a different unit PRTG will automatically convert values internally.
Period	Select the time period for the scale (so you create a scale per time period designation). Choose from the drop down menu: • **Hour** • **Day** • **Week** • **Month** **Scale** and **Period** together define the unit for the given value. If the channel's data is provided in a different unit PRTG will automatically convert values internally.
On Notification	Select a notification that will be triggered if the value in the combined unit (scale per period) is overrun. Choose a notification from the drop down menu. The menu shows all notifications defined in the notifications 825 setup. You can also choose **None** in order to only use other conditions for this trigger.
Delete	Click on the **Delete** button next to an existing notification trigger to delete it. *Note:* It will be deleted immediately and there is no warning message.

No escalation notification, no repeat, and no off notification are available for this trigger type. Click on the **Save** button at the end of the page to store your settings. You can then add another trigger.

Threshold Triggers

Define triggers that will be prompted when certain sensors reach specific values. Click on the **Add Threshold trigger** button to add a new trigger. Then define settings as described below. Every trigger will cause one or more notification(s) to be executed.

Threshold Trigger(s)	
Channel	Select the channel that will be regarded for this trigger from the drop down menu. Select **Primary** to use the sensor's primary channel (this can be defined in the sensor's settings 202) or choose a specific channel name from the list (there are different channels for every sensor type). All following settings for this trigger will be based on the chosen channel.
Condition	Select the condition that will trigger the notification. Choose from the drop down menu: • **Above**: The trigger will be prompted if the value of the selected channel overruns a defined value. • **Below**: The trigger will be prompted if the value of the selected channel undercuts a defined value.

Threshold Trigger(s)	
	• **Equal**: The trigger will be prompted if the value of the selected channel is the same as a defined value. • **Not Equal**: The trigger will be prompted if the value of the selected channel is different than a defined value.
Value	Define the value the channel's data will be compared with. This value will be directly compared to the channel's data. Please enter an integer value.
Latency (sec.)	Define how many seconds will be waited before an **On Notification** is triggered. This can avoid false alarms in case a channel reaches a limit for just a few moments. If the combined condition (channel, condition) persists after the defined time span, the notification will be triggered. Please enter an integer value in seconds.
On Notification	Select a notification that will be triggered if the combined channel condition (channel, value) is true *and* the **Latency** time defined has passed. Choose a notification from the drop down menu. The menu shows all notifications defined in the notifications setup. You can also choose **None** in order to only use other conditions for this trigger.
Off Notification	Select a notification that will be triggered if the combined channel condition (channel, value) is not true any more because the channel's value changes again. **Latency** is not valid for this setting; an **Off Notification** will be sent as soon as the defined condition is not valid any more.You can also choose **None** in order to only use other conditions for this trigger.
Delete	Click on the **Delete** button next to an existing notification trigger to delete it. *Note:* It will be deleted immediately and there is no warning message.

No escalation notification and no repeat are available for this trigger type. Click on the **Save** button at the end of the page to store your settings. You can then add another trigger.

Change Triggers

Define triggers that will be prompted by some sensors whenever certain values have changed. Click on the **Add Change trigger** button to add a new trigger. Then define settings as described below. Every trigger will cause one notification to be executed.

Note: You can enable all sensors to send 'On change' notifications by default when a value changes. To do so, change the **Sensor Value Detection** settings of the Root 166 group settings.

Change Trigger(s)	
Notification	Select a notification that will be triggered whenever a compatible sensor triggers a change notification. It will be executed immediately.

© 2011 Paessler AG

There are no other sensors available for this trigger type. Click on the **Save** button at the end of the page to store your settings. You can then add another trigger.

Sensor Settings Overview

For information about sensor settings, please see the following sections:

- Sensor Settings 202
- List of Available Sensor Types 203

Object Settings Overview

For more general information about object settings, please see section Object Settings 111.

Part VII

Ajax Web Interface—Advanced Procedures

7 Ajax Web Interface—Advanced Procedures

The Ajax-based web interface is your access to PRTG. It is used to configure devices and sensors, and to set up notifications, as well as review monitoring results and create reports. This web interface is highly interactive and uses Asynchronous Java Script and XML (AJAX) to deliver a powerful and easy-to-use user experience. While the user is logged in 93, the data on the screen is permanently refreshed (via Ajax calls) so it always shows the current monitoring results (refresh interval and method can be set 884 by the user).

The following sections introduce more advanced procedures in the Ajax Graphical User Interface (GUI).

Ajax Web Interface—Advanced Procedures—Topics

- Toplists 807
- Arrange Objects 811
- Multi-Edit Sensor Table Lists 813
- Compare Sensors 819
- Geo Maps 823
- Notifications 825
- Reports 827
- Maps 842
- Setup 857

Other Ajax Web Interface Sections

- Ajax Web Interface—Basic Procedures 92
- Ajax Web Interface—Device and Sensor Setup 144

Related Topics

- Windows GUI 894
- Other User Interfaces 926

© 2011 Paessler AG

7.1 Toplists

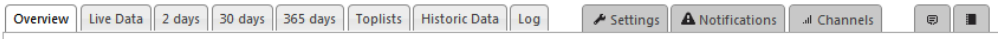
Packet Sniffer and xFlow sensor types can not only measure the total bandwidth usage, they can also break down the traffic by IP address, port, protocol, and other parameters. The results are shown in so-called **Toplists**. This way PRTG is able to tell which IP address, connection, or protocol uses the most bandwidth. PRTG looks at all network packets (or streams) and collects the bandwidth information for all IPs, ports, and protocols. At the end of the toplist period, PRTG stores only the top entries of each list in its database.

Only Top Entries are Stored

Storing all available analysis data in a database during the analysis process would create a huge amount of data which would be very slow to transfer between probe and core and also retrieving data would be too slow. By storing only the top 100 entries for short periods of time it is possible to reduce the amount of data to a minimum while still being able to identify devices with huge bandwidth usage.

Toplists Overview

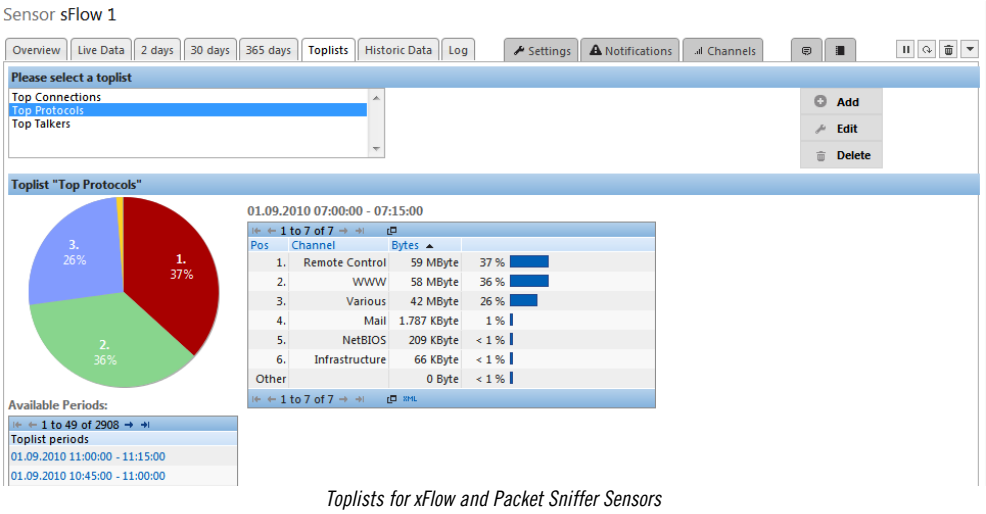
Pages of probes, groups, device, and sensors have a tab-like interface. Using the tabs you can navigate through various sub-pages of an object in order to show your network's status, view monitoring results, or change settings.



Tabs Bar on Sensor Pages

The **Toplists** tab is available for xFlow and Packet Sniffer sensors 203 only. Click on the tab to open a toplist overview. By default, there are three different toplists predefined for each sensor:

- **Top Connections**: Shows bandwidth usage by connection.
- **Top Protocols**: Shows bandwidth usage by protocol.
- **Top Talkers**: Shows bandwidth usage by IP address.



Toplists for xFlow and Packet Sniffer Sensors

Click on one of these lists to view a distribution chart, and a list of source and destination IP and port, protocols, kind of traffic in different channels, etc. It depends on the selected list, which information is available. Click on an entry in the **Available Periods** lists on the left side to view data for a certain time span. By default, a time span of 15 minutes, and a top count of 100 is set. This means, for every list, you can view the top 100 measured in 15 minutes intervals.

You can add or delete new toplists, or edit existing ones.

Add

Click on the **Add** button to create a new toplist. The available options are the same as for editing 808 a list.

Edit

Select a toplist on the left and click on the **Edit** button to modify it.

Toplist Settings	
Name	Enter a meaningful name to identify the toplist.
Type	▪ **Top Talkers (Which IPs uses the most bandwidth?)**: Shows bandwidth usage by IP address. ▪ **Top Connections (Which connections use most bandwidth?)**: Shows bandwidth usage by connection. ▪ **Top Protocols (Which protocols use the most bandwidth?)**: Shows bandwidth usage by protocol. ▪ **Custom (Create your own toplist)**: Create your own list by selecting criteria below.
Toplist is based on	This setting is only available if a custom type is selected above. Select the fields you want to add to the toplist by adding a check mark in front of the respective field name. The available options depend on the type of sensor used. They're different for Packet Sniffer, NetFlow v5, v9, and sFlow. *Note:* For performance reasons, only select the field you really want to monitor. Please see Performance Considerations 809 section below.
Period (Minutes)	Define the interval for the toplist in minutes. Please enter an integer value. Toplists always cover a certain time span. Once a time span has passed, the top results are stored and a new toplist is started. *Note:* In order to avoid load problems on your probe system, please do not set this interval too long. Default setting is **15** minutes. Please see Performance Considerations 809 section below.
Top Count	Define the length of your toplist. Only this number of entries will be stored for each period. Please enter an integer value. *Note:* In order to avoid load problems on your probe system, please do not set this value as low as possible. Default setting is **100**, in order to store the top 100 entries for each period. Please see Performance Considerations 809 section below.

© 2011 Paessler AG

Toplist Settings	
Probe/Core Data Transfer	Define how the probe sends the toplist dataset to the core server. Choose between: ▪ **According to sensor interval (default)**: Send data in the interval defined in the settings of the sensor this toplist is created for. This can create a lot of bandwidth and CPU load with many sniffer sensors, complex traffic, or long toplists. ▪ **Wait until toplist period ends (less cpu&bandwidth usage)**: Send data once a toplist period has finished. This will create less bandwidth usage and CPU load, but you cannot see the *current* toplist in the web interface, but only toplists with finished periods. For more information, please see Performance Considerations 809 section below.
Memory Limit (MB)	Define the maximal amount of memory in MB the probe will use for collecting the different connection information. Every toplist adds its amount to the probe's memory consumption. Increase this value if the number of captured connections is not sufficient. Please enter an integer value.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Delete

Select a toplist on the left and click on the **Delete** button. Confirm with **Yes** to delete the list.

Performance Considerations

If you create toplists for data lines with considerable usage (e.g. steady bandwidth over 10 Mbit/s) or if the traffic is very diverse (i.e. many IPs/ports with only little traffic each) please consider the following aspects:

- The probe gathers all information needed for the toplist in RAM memory during each period. Only the top 100 entries are transferred to the core. Depending on the toplist type and traffic patterns the required memory can grow into many megabytes.
- Choose periods as short as desirable (especially important when traffic has a high level of diversity) to minimize memory usage.
- Memory requirements can grow almost exponentially with each field used in the toplists definition (depending on traffic pattern). Avoid complex toplists for high and diverse traffic. For example, **Top Connections** (5 fields) needs a lot more memory than **Top Talkers** (1 field).
- If you experience high bandwidth usage between core and probe try to choose the **Wait until toplist period ends** option.
- If you experience *Data incomplete, memory limit was exceeded* messages try to increase the memory limit in the toplist's settings but keep an eye on the probe process' memory usage.

Notes

- When working with toplists be aware that privacy issues can come up for certain configurations of this feature. Using toplists you can track all single connections of an individual PC to the outside world and you, as the administrator, must make sure that it is legal for you to configure PRTG like this.
- Keep in mind that toplists can be viewed through the web interface. You may not want to show lists of domains used in your network to others. So you should restrict access to sensor types having toplists.

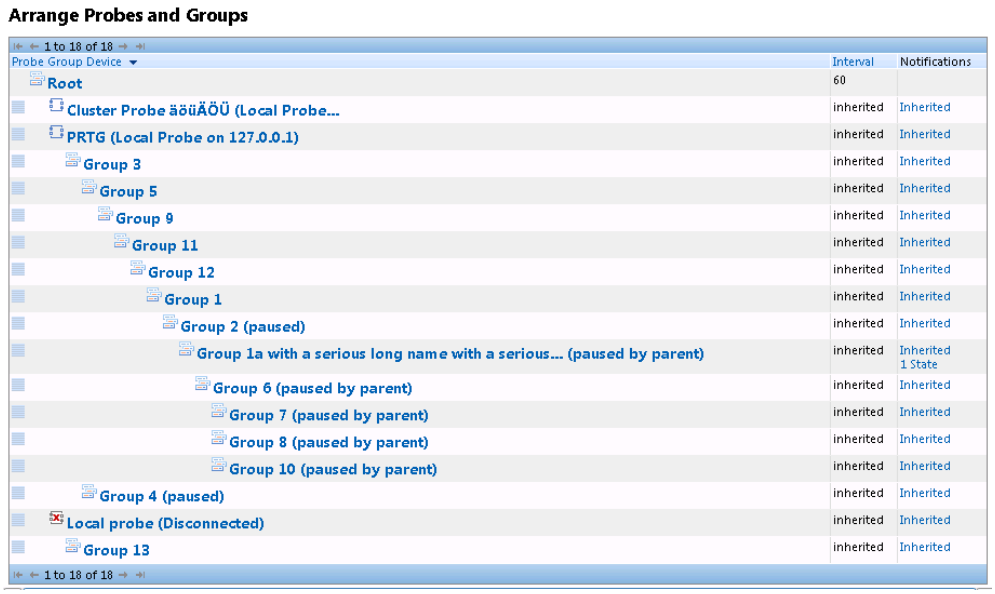
© 2011 Paessler AG

7.2 Arrange Objects

There are several possibilities to move objects within the device tree, or to move objects from one probe or group to another.

Arrange Probes and Groups

From the main menu, select **Devices | Arrange Probes & Groups** to open a page with a tree-like view of all probes and groups of your setup.



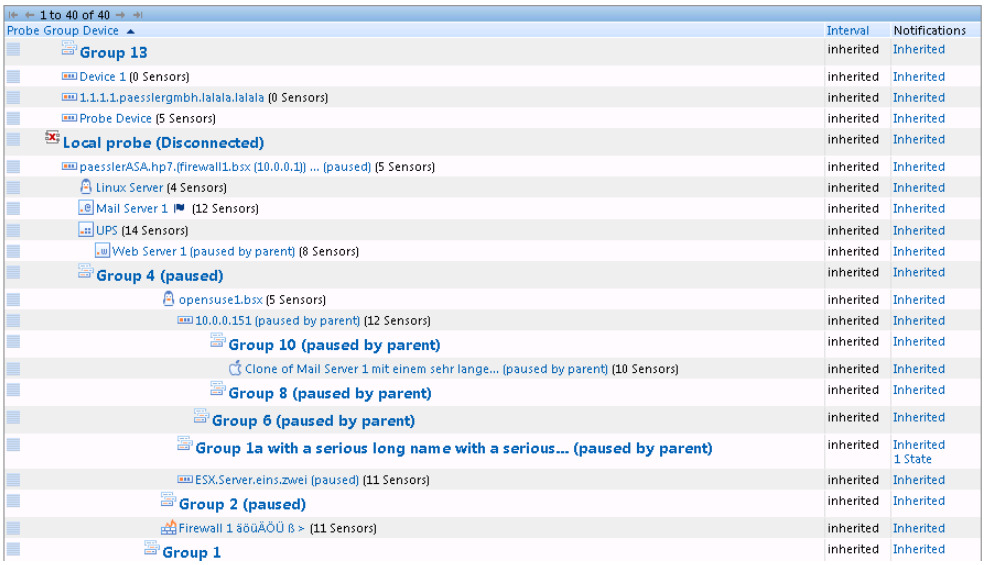
Arrange Probes and Groups

Click on the column headers **Probe Group Device** to resort the tree upside-down, or click on the **Interval** column to sort by the interval set for the objects. To move a probe or group, simply click on the small grip at the beginning of the row and drag it to the position you like. This way, you can change the order of objects, and even make an object another parent's child. Changes take effect immediately.

Arrange Groups and Devices

From the main menu, select **Devices | Arrange Groups & Devices** to open a page with a tree-like view of all groups and their devices in your setup.

Arrange Groups and Devices


1 to 40 of 40
Probe Group Device
Interval
Notifications
Group 13
Device 1 (0 Sensors)
1.1.1.1.paesslergmbh.lalala.lalala (0 Sensors)
Probe Device (5 Sensors)
Local probe (Disconnected)
paesslerASA.hp7.(firewall1.bsx (10.0.0.1)) ... (paused) (5 Sensors)
Linux Server (4 Sensors)
Mail Server 1 (12 Sensors)
UPS (14 Sensors)
Web Server 1 (paused by parent) (8 Sensors)
Group 4 (paused)
opensuse1.bsx (5 Sensors)
10.0.0.151 (paused by parent) (12 Sensors)
Group 10 (paused by parent)
Clone of Mail Server 1 mit einem sehr lange... (paused by parent) (10 Sensors)
Group 8 (paused by parent)
Group 6 (paused by parent)
Group 1a with a serious long name with a serious... (paused by parent)
ESX.Server.eins.zwei (paused) (11 Sensors)
Group 2 (paused)
Firewall 1 äöüÄÖÜ ß > (11 Sensors)
Group 1
inherited
Inherited
1 State

Arrange Groups and Devices

Click on the column headers **Probe Group Device** to resort the tree upside-down, or click on the **Interval** column to sort by the interval set for the objects. To move a group or device, simply click on the small grip at the beginning of the row and drag it to the position you like. This way, you can change the order of objects, and even make an object another parent's child. Changes take effect immediately. *Note:* **Probe Device** and **Cluster Probe Device** are immovable.

Move via Context Menu

As alternative, you can also use an object's context menu to move it. For more information, see section Context Menus 124.

© 2011 Paessler AG

7.3 Multi-Edit Lists

Device and sensor tables, as well as some other lists (e.g. for maps or reports) offer multi-edit functionality. With this, you can bulk edit the properties of many objects at a time. *Note:* Using multi-edit, not all settings can be changed, but only a limited selection of functionalities are provided.

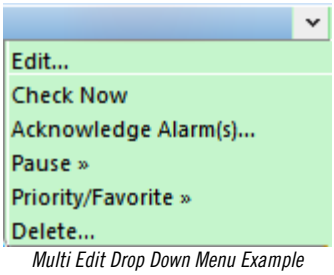
Start of List Example

In a table, start multi-edit by selecting objects using the check boxes on the right. You can also select all objects of the current page by clicking the check box in the table header. As soon as you select one or more objects, a green multi-edit menu appears at the top of the table.

Multi Edit Menu

Depending on the object type different functions are available. For example, for sensor lists, some frequently used functions are available as quick buttons, such as **Delete**, **Pause**, **Resume**, **Check Now**, and **Edit**.

Other options are available in the drop down menu. *Hover* the arrow symbol to show this. The content of the menu varies depending on the kind of objects selected. When editing, you can only change the settings that are common for all selected objects.



Multi Edit Drop Down Menu Example

Related Topics

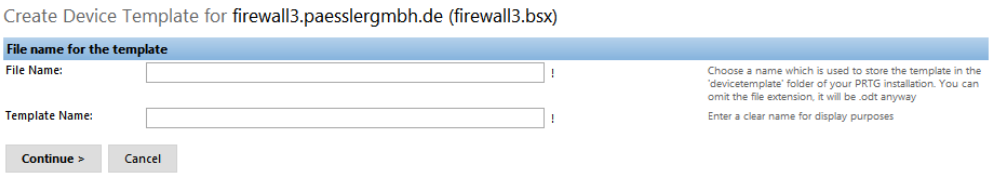
- Working with Table Lists 119

© 2011 Paessler AG

7.4 Create Device Template

If you want to add a certain device several times, you can create a device template from an existing device in your device tree. When creating a device template, information for nearly all sensors on this device will be saved to a template file which you can later use in combination with Auto-Discovery 145 (restrictions apply for a few sensor types). From the sensors, all relevant settings will be saved, except those that refer to other objects, such as schedules, triggers, access rights, etc. They will automatically be reverted to **Inherit**.

To start, right click on a device in your sensor tree, and from the context menu 124, select **Create Device Template...**. An assistant will appear.


Create Device Template for firewall3.paesslergmbh.de (firewall3.bsx)
File name for the template
File Name:
Choose a name which is used to store the template in the 'devicetemplate' folder of your PRTG installation. You can omit the file extension, it will be .odt anyway
Template Name:
Enter a clear name for display purposes
Continue >
Cancel

Creating a Device Template

Device Template Settings

File name for the template	
File Name	Enter a name under which the file will be stored. It will be stored with the extension *.odt* in the *\PRTG Network Monitor\devicetemplates* sub-directory of your PRTG core installation (of the Master node, if in a cluster). The file may not exist in this directory, otherwise you will see an error message.
Template Name	Enter a meaningful display name for the template, as it will appear in the web interface.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

You should see a success message indicating that your template file was saved. Finished! The device template is now stored in the program path of your PRTG core installation. Your device template file contains all sensors, including their settings, of the original device.

During your next auto-discovery, choose the **Automatic sensor creation using specific device template(s)** option and select the name of your newly created device template from the list. PRTG will then try to discover the stored sensor types on the new (or existing) device. If the physical device answers to a sensor request, the sensor is added to the PRTG device. *Note:* Numbers will be added to the original sensor names. For detailed information, please see Auto-Discovery 145 section.

Settings That are Not Saved

There are a few settings which cannot be saved into a device template, and will therefore be set to default, such as the *Dependency Type* setting **Master object for parent** (in **Schedules and Dependencies** section), and *Result Handling* settings **Write result do disk** (as this is intended for debugging purposes only). Also, settings in the **Access Rights** section are not saved to avoid security flaws.

Furthermore, due to internal restrictions, the following sensor types will not be saved into a device template:

- **Core/Probe/Cluster Health**
- **DHCP**
- **HDD Health**
- **jFlow V5**
- **jFlow V5 (Custom)**
- **NetFlow V5**
- **NetFlow V5 (Custom)**
- **NetFlow V9**
- **NetFlow V9 (Custom)**
- **Packet Sniffer (Content)**
- **Packet Sniffer (Custom)**
- **Packet Sniffer (Header)**
- **QoS (Quality of Service)**
- **Sensor Factory**
- **sFlow**
- **sFlow (Custom)**
- **SNMP Trap Receiver**
- **Syslog Receiver, SNMP Trap Receiver**
- **WMI Free Disk Space (Single Disk)** (use WMI Free Disk Space (Multi Drive) Sensor 711 instead)

Related Topics

- Clone Object 817

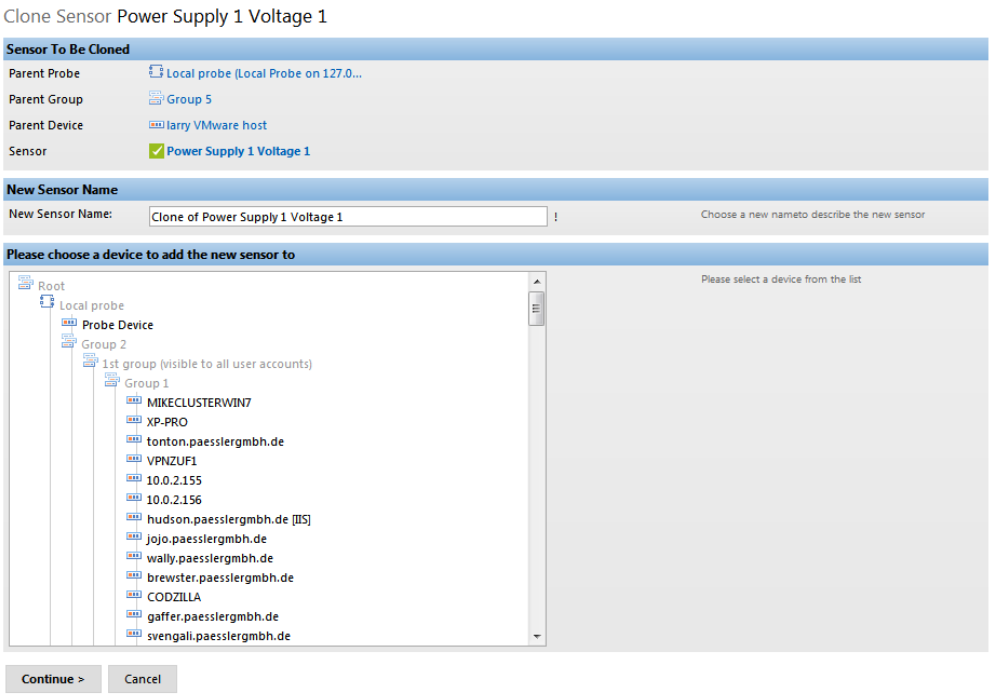
© 2011 Paessler AG

7.5 Clone Object

If you want to duplicate an object with the same settings, you can clone it. Cloning is available for groups, devices, and sensors. Unlike the results when using the Create Device Template 815 option, a cloned device will contain all objects of the original device, regardless of whether they bring about working sensors or not (which often depends on the settings of the cloned device).

Note: You cannot clone 'fixed' objects, such as the root group or a probe device.

To start, right click on an object in your device tree, and from the context menu 124, select **Clone...**. An assistant will appear.



Cloning a Sensor

Clone Object Settings

Object **To Be Cloned**	
Object	Several fields show information about the object that is to be cloned. The available information varies depending on whether you are about to clone a group, device, or sensor.

New *Object's* **Name**	
New *Object* **Name**	Enter a name for the cloned object. By default, the old name is filled in, proceeded by *Clone of*.

New *Object's* Name	
New IP Address/DNS Name	This field is only available when cloning a device. Enter the IP address or DNS name for the new device.

Please choose a group/device to add the new *object* to
From the device tree shown, choose an object you want to add the cloned object to. When cloning a group or device, select a group. When cloning a sensor, select the device you want to add it to.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

You will be redirected to the newly cloned object's overview 104 page. By default, all sensors are initially paused to give you the chance to change settings before monitoring starts. Please check the settings 111 and resume 123 monitoring.

Related Topics

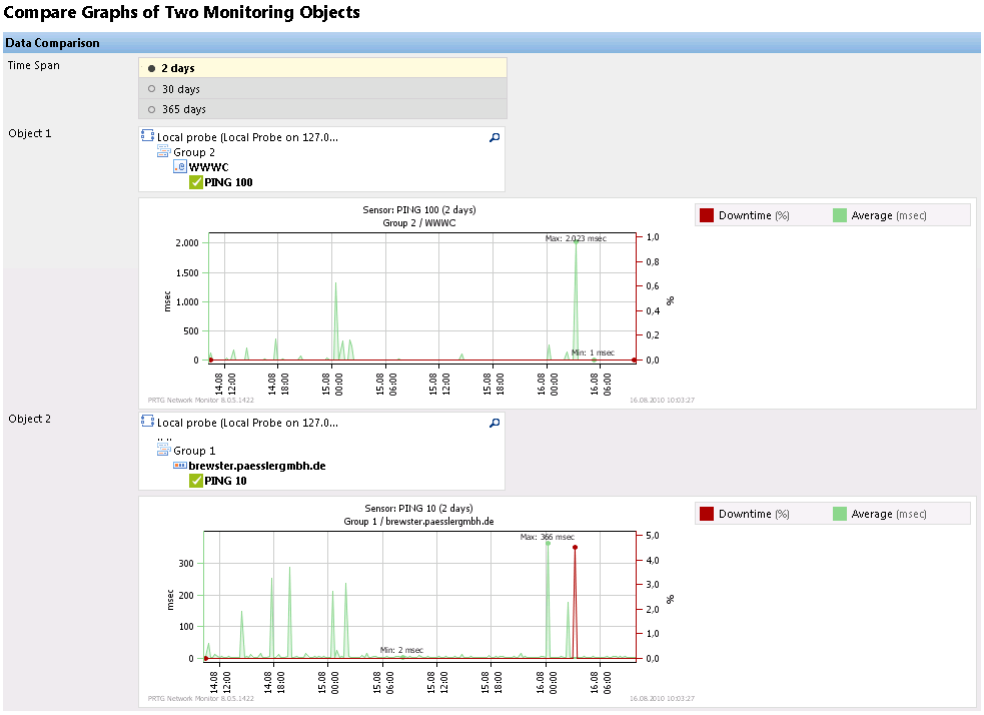
- **Create Device Template** 815

© 2011 Paessler AG

7.6 Compare Sensors

This function allows you to visually compare the graphs of two specific objects. The two graphs will be shown next to each other so you can have a look at both of them at the same time.

To open the page to compare graphs of two monitoring objects, from the main menu, choose **Sensors | Compare Sensors**.



Compare Graphs of Two Monitoring Objects

Compare Sensors Settings

Data Comparison	
Time Span	Specify the time span for which you want to show the graphs for. Choose between: ▪ **2 days** ▪ **30 days** ▪ **365 days**
Object 1	Select the first object you want to show a graph for. Click on the reading-glass symbol to open the Object Selector 120.
Object 2	Select the second object you want to show a graph for. Click on the reading-glass symbol to open the Object Selector 120.

The graphs will be shown immediately after object selection.

Related Topics

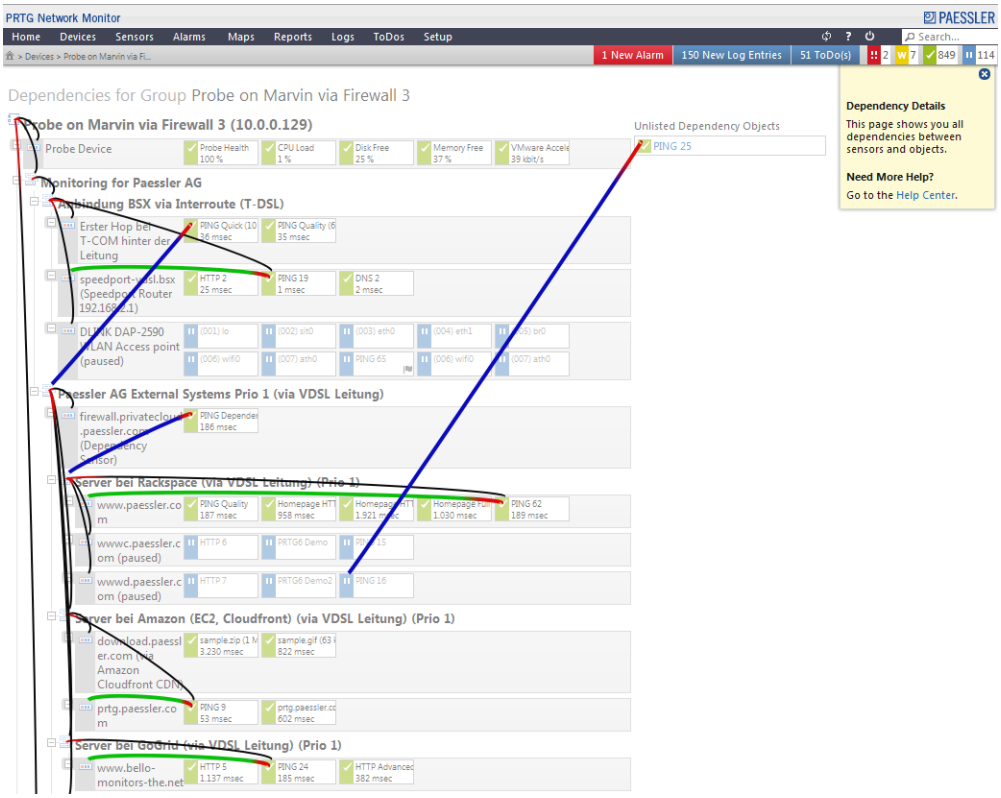
If you want to create a sensor that combines the data of different other sensors, please see
- Sensor Factory Sensor 497

© 2011 Paessler AG

7.7 Show Dependencies

This function shows an overview of the dependencies configured for the objects in your setup. For a general introduction please see Dependencies 85 section.

In the main menu, choose **Devices**, and then *hover* the menu item **Dependencies** to show other menu items. Follow the menu path (it is specific to your setup) to view dependencies of the objects in a specific probe or group only.



Dependency View

You will see the device tree shown in the background, with lines of different color connecting objects. The lines symbolize dependencies between objects. Additionally, a color code is used.

Color Code

The line's colors show the kind and source of a dependency.

- **Black**
  Black lines show a dependency by inheritance (*Use parent*). The source of the dependency is shown with a line's end in **Red** color.

- **Blue**
  Blue lines show a dependency that was set manually (*Select object*). The source of the dependency is shown with a line's end in **Red** color.

- **Green**
  Green lines show a master dependency for a device (*Master object for parent*). The sensor which is set as master is shown with a line's end in **Red** color.

© 2011 Paessler AG

7.8 Geo Maps

For each probe, group, or device, you can enter **Location** information. PRTG will use the first line of this information to query a Google Map which shows your objects on a geographical map. After entering your personal *Google Maps API Key* (you can sign up for free) you can start using geo maps right away by adding location information to your devices, e.g. in the **Root** 166 group for a start.

Example of Geo Maps in PRTG Ajax Web Interface

In order to use geographical maps within the PRTG web interface 92 or Windows GUI 894, please make sure the following:

1. Apply for a Google Maps API key on the Google Code website. This will only take a few minutes. For detailed information, please see **More** section below.

2. In the system administration (within the web interface), select the maps type you want to view. There, you will also find an option to disable Google Maps integration if you do not want to use it. Paste your API key there. See section **System Administration—System and Website** 871 (setting **Geo Maps**) for detailed information.

3. In your objects' settings 111, add a city name or address in the first line of the **Location** field. As soon as you view the details of such an object, a geographical map will be shown. The **Location** information will also be used when viewing objects in the **Windows GUI** 894 or when adding **Geo Maps** objects to PRTG **Maps** 842.

More

Knowledge Base: How do I get an API Key in order to use Google Maps with PRTG?
- http://www.paessler.com/knowledgebase/en/topic/17093

Knowledge Base: I would like to see interactive Google Maps for PRTG's Geo Map feature
- http://www.paessler.com/knowledgebase/en/topic/7903

Knowledge Base: Can I avoid the "page contains insecure content" popups for PRTG 8 Geo Map feature?
- http://www.paessler.com/knowledgebase/en/topic/7333

Knowledge Base: Which limitations apply when using the Google Maps API in PRTG?
- http://www.paessler.com/knowledgebase/en/topic/7913

Knowledge Base: Why do I see a "Sorry, can not show all items in this map" note on my Geo Maps?

- http://www.paessler.com/knowledgebase/en/topic/9153

© 2011 Paessler AG

7.9 Notifications

Notifications are used to send alerts to the user whenever PRTG discovers a defined state, such as slow or failing sensors, or when threshold values are breached. You can define an unlimited number of notifications allowing to use one, or more, of several communication channels like email, pager, SMS text messaging, and many more. For video instructions, please see the More 826 section below.

Overview

Notifications can be triggered by:

- **Sensor status changes**
  For example, when a sensor changes status to **Up** or **Down**, if responses are slow or sensors show an **Unusual** status.

- **Sensor value threshold breaches**
  For example, when a sensor shows a request time higher than 1,000 ms for more than 30 minutes.

- **Speed threshold breaches**
  For example, when a traffic sensor shows more than 1 Mbit/s for more than 5 minutes.

- **Volume threshold breaches**
  For example, when a traffic sensor shows more than 1 Gbyte transferred in 24 hours.

- **Sensor value changes**
  For some sensors you can trigger a notification whenever the value changes, for example, when monitoring files on a hard disk drive.

A notification can be one of these actions:

- Send Email
- Add Entry to Event Log
- Send Network Broadcast (NET SEND)
- Send Syslog Message
- Send SNMP Trap
- Send SMS/Pager Message
- Execute HTTP Action
- Execute Program

Notifications contain valuable sensor information, such as:

- Last error message
- Last good/failed request
- Total downtime
- Total uptime
- Recent sensor history

© 2011 Paessler AG

Notifications Setup

There are three steps to take in order to use notifications with PRTG. Please go through all of them:

1. Check and set up the **Notification Delivery** settings. This will tell PRTG how to send messages. See section System Administration—Notification Delivery 877 for detailed information.

2. Check and set up several **Notifications**. This will define the kind of message and its content. See section Account Settings—Notifications 862 for detailed information.

3. Check and set up **Notification Triggers** for objects. These will prompt the defined notifications. See section Sensor Notifications Settings 797 for detailed information.

More

Video Tutorial: There is a video available on the Paessler video tutorials page.

- http://www.paessler.com/support/video_tutorials

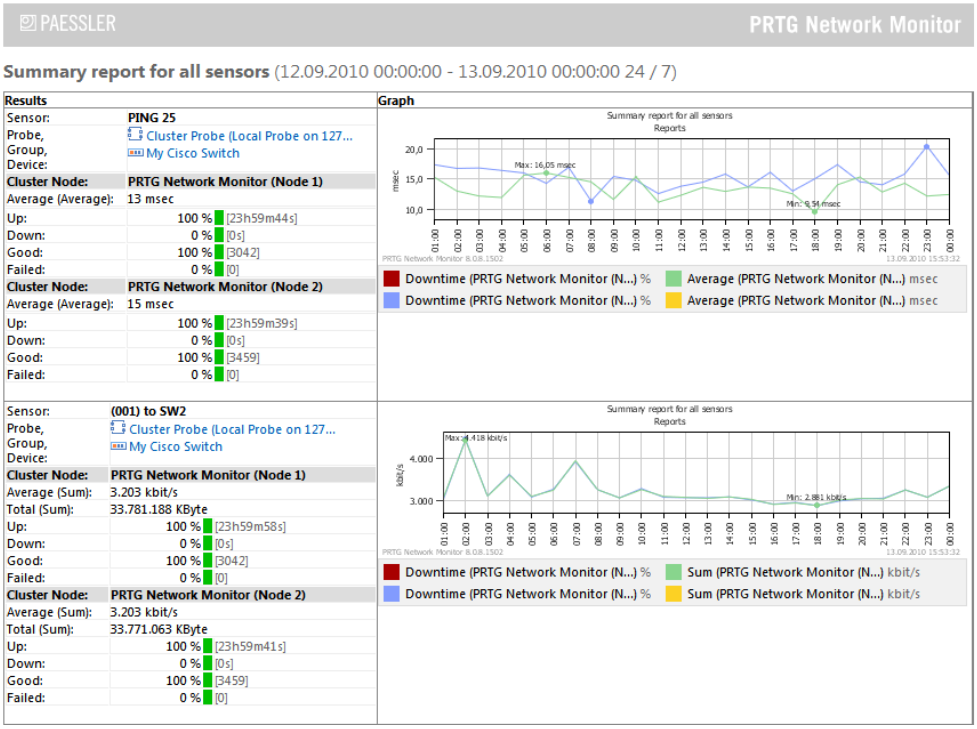
© 2011 Paessler AG

7.10 Reports

Reports are used to analyze historic monitoring results over a specified time such as one or more days, one month, or an entire year. You can create reports for all, or only for certain sensors.

Introduction

PRTG includes a powerful reporting engine for ad-hoc, as well as scheduled report generation in HTML and PDF format. Thus, reports can be run on demand or on a regular basis (e.g. once a day). You can create reports for one single sensor, or you choose a range of sensors you want to create a report for. The content and layout of the report is controlled by the report template of your choice and is the same for all sensors in a report.


PAESSLER
PRTG Network Monitor
Summary report for all sensors (12.09.2010 00:00:00 - 13.09.2010 00:00:00 24 / 7)
Results
Graph
Sensor: PING 25
Probe, Group, Device: Cluster Probe (Local Probe on 127...
My Cisco Switch
Cluster Node: PRTG Network Monitor (Node 1)
Average (Average): 13 msec
Up: 100 % [23h59m44s]
Down: 0 % [0s]
Good: 100 % [3042]
Failed: 0 % [0]
Cluster Node: PRTG Network Monitor (Node 2)
Average (Average): 15 msec
Up: 100 % [23h59m39s]
Down: 0 % [0s]
Good: 100 % [3459]
Failed: 0 % [0]
Summary report for all sensors
Reports
Max: 16.05 msec
Min: 6.94 msec
msec
Downtime (PRTG Network Monitor (N...) %
Average (PRTG Network Monitor (N...) msec
Sensor: (001) to SW2
Probe, Group, Device: Cluster Probe (Local Probe on 127...
My Cisco Switch
Cluster Node: PRTG Network Monitor (Node 1)
Average (Sum): 3.203 kbit/s
Total (Sum): 33.781.188 KByte
Up: 100 % [23h59m58s]
Down: 0 % [0s]
Good: 100 % [3042]
Failed: 0 % [0]
Cluster Node: PRTG Network Monitor (Node 2)
Average (Sum): 3.203 kbit/s
Total (Sum): 33.771.063 KByte
Up: 100 % [23h59m41s]
Down: 0 % [0s]
Good: 100 % [3459]
Failed: 0 % [0]
Max: 4.418 kbit/s
Min: 2.881 kbit/s
kbit/s
Sum (PRTG Network Monitor (N...) kbit/s

Report Sample

The sample above shows a report for a router device. You can see graphs for the last day, plus data tables with numeric results.

Start Reports

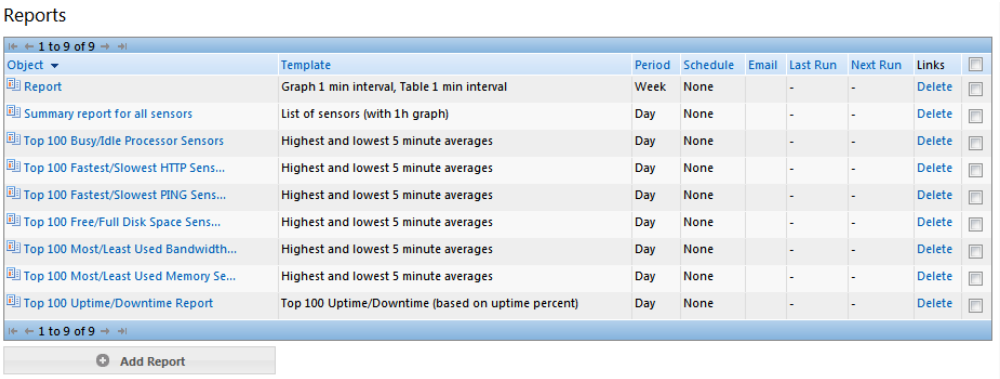
Click the **Reports** entry from the main menu [137] to view or add reports of your monitoring data. *Hover* to show other menu items. Choose between:

- **All**
  Calls the Reports feature where you can view or add reports of your monitoring data.

- **Add Report**
  Lets you directly add a new report.

- **Select Report ›**
  Show existing reports. *Hover* to show other menu items. Follow the menu path (it is specific to your setup) to select a report.

Reports Overview



In the **All** view, you see a list of all existing reports. Every line shows information about one report:

- **Period**: The time span covered by the report.
- **Schedule**: Shows if a schedule is set to regularly execute the report automatically.
- **Email**: If a schedule *and* an email address is set in the report settings, this shows the email address the report is automatically sent to.
- **Last Run**: If a schedule is set in the report settings, this shows when the report was last run.
- **Next Run**: If a schedule is set in the report settings, this shows when the report will be run next.

Using the **Delete** link at the end of a line you can delete the report.

Please see also Working with Table Lists 119. Additionally, there is multi-edit available. This enables you to change properties of several objects at a time. For more details, please see Multi-Edit Lists 813 section.

Click on the **Add Report** button to add a new report, or click on the name of an existing report to view and edit its settings. You can also run a pre-configured report easily by clicking on its name and then using the options in the **Run Now** tab. For both options, please see Reports Step By Step 830 section.

Working With Reports

For detailed information on how to create, edit, and schedule reports, please see the following sections:

- Reports Step By Step 830
- View and Run Reports 833
- Reports Settings 835

© 2011 Paessler AG

Automatic Averaging

For performance reasons, PRTG automatically averages monitoring data when calculating data for large time spans. Data is then averaged regardless of the selected average interval.

Time Span in Report	Minimum Level of Detail (Average Interval)
Up to 40 days	Any
40 to 500 days	60 minutes/1 hour or larger

A report for a time span of more than 500 days is not possible. If you try to set a larger time span, it will be reduced to 365 days automatically.

Related Topics

- Review Monitoring Data 104
- Historic Data Reports 107

7.10.1 Reports Step By Step

In order to create a new report, or run an existing one, follow the steps in this section. In the web interface, click on the **Reports** entry in the main menu to show the reports main screen.

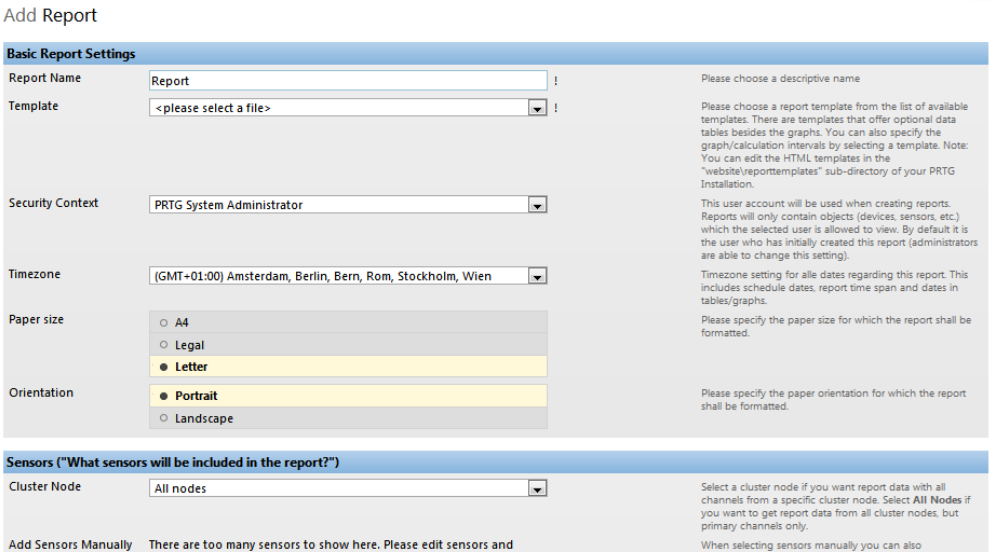
Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Quick Start: Run an Existing Report

PRTG is delivered with several pre-configured reports. In order to use one of them, click on a report's name in the reports main screen, select the **Settings** tab. The other steps are the same as for new reports. Although some settings are already given, we recommend checking the settings. For example, check the sensors that will be included in the report. For some reports that come with PRTG there are no sensors added yet. Continue with Step 3 831 in this section.

Step 1: Add Report

Click on the **Add Report** button to add a new report. An assistant is shown. You can define many settings. For a beginning, enter a **Report Name**.


Add Report
Basic Report Settings
Report Name
Report
Please choose a descriptive name
Template
<please select a file>
Please choose a report template from the list of available templates. There are templates that offer optional data tables besides the graphs. You can also specify the graph/calculation intervals by selecting a template. Note: You can edit the HTML templates in the "website\reporttemplates" sub-directory of your PRTG Installation.
Security Context
PRTG System Administrator
This user account will be used when creating reports. Reports will only contain objects (devices, sensors, etc.) which the selected user is allowed to view. By default it is the user who has initially created this report (administrators are able to change this setting).
Timezone
(GMT+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
Timezone setting for alle dates regarding this report. This includes schedule dates, report time span and dates in tables/graphs.
Paper size
A4
Legal
Letter
Please specify the paper size for which the report shall be formatted.
Orientation
Portrait
Landscape
Please specify the paper orientation for which the report shall be formatted.
Sensors ("What sensors will be included in the report?")
Cluster Node
All nodes
Select a cluster node if you want report data with all channels from a specific cluster node. Select All Nodes if you want to get report data from all cluster nodes, but primary channels only.
Add Sensors Manually
There are too many sensors to show here. Please edit sensors and
When selecting sensors manually you can also

Add Report Assistant

Step 2: Select a Template

In the **Template** section, select one of the report templates from the list. This will define the overall look of your report and affect in which detail (interval) monitoring data is included. For a detailed description on the available options, please see Reports Settings 835 (Settings—Template) section. If you're not sure, try with a template that appears suitable to you. You can change all settings later.

© 2011 Paessler AG

Step 3: Define Additional Settings

Select a **Security Context** (best choose **PRTG System Administrator**, if available), your **Timezone**, and **Paper Size** and **Orientation** for PDF generation. For detailed information, please see Reports Settings 835 (Settings) section.

Step 4: Select Nodes and Sensors

Choose the sensors you want to include in the report. First, define the **Cluster Node** the monitoring data will be taken from. Select a specific node from the list. If you select **All nodes**, a report with data from all of your cluster nodes will be created, but only the primary channel of every sensor will appear in the report.

Every report will show monitoring results from sensor data. There are two ways to include sensors in a report: You can either add sensors manually, or by tag. In the **Add Sensors by Tag** field, enter a tag that matches the sensor range you want a report for. For example, enter the tag *bandwidthsensor* to include all sensors that measure bandwidth. PRTG suggests this tag as default when adding bandwidth sensors; so this tag typically gathers all bandwidth sensors, unless you haven't configured your system differently. You can enter several tags separated by space or comma. Use the **Exclude Sensors by Tag** field to explicitly remove sensors with certain tags from the bulk of tags defined above.

Tagging is a great tool to group sensors or other objects. For more information, see Tags 84 section. You can also leave the tag fields empty and only choose specific sensors manually later.

Step 5: Decide On a Schedule and Additional Settings

In the **Report Schedule** section, choose if you want to run the report on a regular basis or on demand only. Also choose which time **Period** will be covered by the report, and if you want to show percentiles, add report comments, or special access rights. For detailed information, please see Reports Settings 835 (Settings) section.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Step 6: Check and Adjust the Sensors Included

When settings are saved, switch to the **Sensors Selected by Tag** tab to see a list of all sensors that were added by the tag(s) you defined in step 4. To change tags, go back to the **Settings** tab. You can additionally add sensors manually. To do so, switch to the **Select Sensors Manually** tab. See Reports Settings 840 (Select Sensors Manually) section for detailed information. The final report will show sensors from both manual and by tag selection.

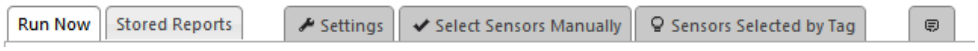
Step 7: Run Report

Switch to the **Run Now** tab, select the current or previous period, and in the **Processing Options** select **View Report as HTML**. Click the **Run Report** button. The report will be generated in a new browser window or tab immediately. Depending on the number of selected sensors and the used template it may take a few minutes until you see the report. If you do not want to wait, close the newly opened browser window or tab and select a PDF option in the **Processing Options**. Click on the **Run Report** button again. The report will then be generated in the background and you will get a ToDo 117 or email once it's finished.

© 2011 Paessler AG

7.10.2 View and Run Reports

In the web interface, click on the **Reports** entry in the main menu to show the reports main screen. Click on a report's name to select it. Using the reports tabs you can access all functionalities and settings for this report. Click on the **Go to all reports** button at the bottom of the page to return to the list of Reports.



Reports Tabs

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Run Now

In the **Run Now** tab you can execute a report immediately with the settings configured.

Run Report "*[Name]*"	
Report for	Define the time span covered by the report. Choose between: ▪ **Current Period**: Use monitoring data of the current period. The actual time span depends on the report period type defined in the report's settings 835. It can be today, this week, this month, or this year. ▪ **Previous Period**: Use monitoring data of the last period. The actual time span depends on the report period type defined in the report's settings 835. It can be yesterday, last week, last month, or last year. ▪ **Select A Period**: Use monitoring data of a period other than current or previous. Select below. ▪ **Select Date Range Manually**: Define a custom time span for the monitoring data that will be used. Set start and end date below.
Date Range	This selection is only visible if the period option is enabled above. From the list, select a data range for which the report will be generated. The actual time spans shown depend on the available monitoring data and on the report period type defined in the report's settings 835. It can be days, weeks, months, or years.
Start Date	This selection is only visible if the date range option is enabled above. Define the begin of the time span for which the report will be generated. Click in the field and select a data from the calendar. Make sure you define a valid period.
End Date	This selection is only visible if the date range option is enabled above. Define the end of the time span for which the report will be generated. Click in the field and select a data from the calendar. Make sure you define a valid period.

Processing Options	
File Format and Delivery	Define how you want to view the report. Choose between: ▪ **View Report as HTML**: Directly view the report in your web browser. It will be loaded in a new browser window or tab. ▪ **Create and store PDF file**: Create a PDF file of the report and store it. Once finished, you will find it in the **Stored Reports** tab and a ToDo 117 will be created which usually sends out a notification mail to the administrator. ▪ **Create PDF file, store it and send by email**: Create a PDF file of the report, store it, and send it via email once it is finished.
Target Email Address	This option is only visible if sending by email is selected above. Please enter a valid email address the report will be sent to. Email configuration can be changed in the System Administration—Notification Delivery 877 settings.

Click on the **Run Report** button to start report generation. Depending on the number of selected sensors, this may take a while. If you experience a long waiting time when generating HTML reports for immediate view, please consider using one of the PDF options. You can then view the report as soon as it's finished.

Stored Reports

In the **Stored Reports** tab you can view PDF reports created in the past. Simply click on a name to open the report. Reports are stored until they are deleted according to the data purging settings of your PRTG configuration. You can set data purging limits for reports in the System Administration—System and Website 871 settings.

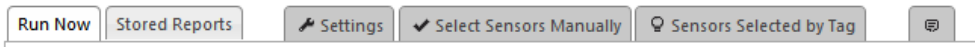
Other Tabs

For all other tabs, please see Reports Settings 835 section.

© 2011 Paessler AG

7.10.3 Reports Settings

In the web interface, click on the **Reports** entry in the main menu to show the reports main screen. Click on a report's name to select it. Using the reports tabs you can access all functionalities and settings for this report. Click on the **Go to all reports** button at the bottom of the page to return to the list of Reports.



Reports Tabs

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Run Now

In the **Run Now** tab you can execute a report immediately with the settings configured. Please see View and Run Reports 833 section.

Stored Reports

In the **Stored Reports** tab you can view reports created in the past. Please see View and Run Reports 834 section.

Settings

Click on the **Settings** tab to open a report's settings.

Basic Report Settings	
Report Name	Enter a meaningful name to identify this report.
Template	Select a template for the report. This will define the overall look of your report. There are several report templates delivered with PRTG. They also define in which detail (interval) monitoring data is included. You can choose from templates in the following categories: ▪ **Graph with Data Table**: Create a report with graphs and data table. Choose from several intervals. ▪ **Data Table Only**: Create a report with data tables only. Choose from several intervals. ▪ **Graph Only**: Create a report with graphs only. Choose from several intervals. ▪ **List of Sensors**: Create a report in a compact sensor list style. This is available with and without graphs. ▪ **Top 100 Highest and Lowest**: Create a report with up to 100 objects with the highest and lowest average values. Choose from different intervals.

Basic Report Settings	
	▪ **Top 10 Uptime/Downtime**: Create a report with up to 10 objects with the highest uptime and downtime each. You can choose between data in percent and hours. ▪ **Top 100 Uptime/Downtime**: Create a report with up to 100 objects with the highest uptime and downtime each. You can choose between data in percent and hours. Monitoring data within an interval is averaged. See also the comment on data averaging in the Reports 829 (Automatic Averaging) section. For information on how to modify templates, please see More 841 section below.
Security Context	Define the user account that will be used for access to monitoring data. The report will only contain objects which the selected user 89 is allowed to view. Please choose a user from the list. The available users depend on your configuration. By default, this is the user that created the report. PRTG Administrator users can change this setting.
Timezone	Define the time zone that will be used for all date-specific settings in this report (see below). Select a time zone from the list.
Paper Size	Define the paper size in which PDF reports will be created. Choose between: ▪ **A4**: Use German DIN A4 format. ▪ **Legal**: Use US legal paper format. ▪ **Letter**: Use US letter paper format.
Orientation	Define the paper orientation in which PDF reports will be created. Choose between: ▪ **Portrait** ▪ **Landscape**

Sensors	
Cluster Node	Define the cluster node the report will take monitoring data from. Choose a cluster node from the list. The available options are specific to your configuration. Select **All nodes** to create a report with data from all of your cluster nodes. *Note:* A report for all nodes will include data of the primary sensor channels only, not for other sensor channels.
Add Sensors Manually	If you want to manually choose the sensors included in this report, please save settings and switch to the Select Sensors Manually 840 tab.

© 2011 Paessler AG

Sensors	
Add Sensors by Tag	Define the sensors included in this report by tag. Enter one or more tags separated by space or comma. The report will cover all sensors that have at least one of the tags. Please enter a string or leave the field empty. *Note:* Tags are inherited 84 invisibly and automatically. So, for example, if you enter the tag of a group here, the report will include all sensors within this group. For detailed information, see **Inheritance of Settings** 82 section. For sensors that are added by tag, all sensor channels are included in the report automatically, except **All nodes** is selected in the **Cluster Node** selection above.
Filter Sensors by Tag	Further filter sensors. This is used in combination with sensors that are added manually, or added implicitly with their manually added parent objects. From those sensors, only the ones with the tags entered here will be included. Enter one or more tags separated by space or comma to include sensors in the report. Please enter a string or leave the field empty.

Schedule	
Report Schedule	Define when the report will be run. Choose between: ▪ **No schedule (run interactive/on-demand only)**: Only use the options in the **Run Now** tab to start generation of this report manually. ▪ **Every full hour**: Run this report every 60 minutes. ▪ **Every day at a specific hour**: Run this report every 24 hours. ▪ **Every specific day of a week**: Run this report every 7 days. Specify the day below. ▪ **Every specific day of a month**: Run this report on a specific day every month. Specify below. ▪ **Every specific date**: Run this report on a specific date every year. Specify below.
Specify Hour	This setting is only visible if specific hour is selected above. From the list, please select the hour you want to run the report at. PRTG will automatically choose a suitable time within this hour, usually at the beginning of it.
Specify Day	This setting is only visible if the day of week or day of month option is selected above. From the list, please select a day of week or a date of the month you want to run the report. When selecting **Last**, the report will always run on the last day of the month, regardless of how many days the month has. When selecting a date that does not exist in every month, e.g. the 30th in May, PRTG will automatically run the report on the last day of this month.
Specify Date	This setting is only visible if the specific date option is selected above. Please enter a valid date in the form **DD.MM**, e.g. *31.12.* The report will be run annually on this date.

Schedule	
Scheduled Processing	This setting is only visible if one of the schedule options is selected above. Define what will be done when generating a report. Choose between: ▪ **Save report to disk and send it by email**: Create a PDF file of the report, store it, and send it via email. You will find the report in your emails and in the **Stored Reports** tab. Define an email address below. ▪ **Save report to disk only**: Create a PDF file of the report and store it. Once finished, you will find it in the **Stored Reports** tab and a ToDo 117 will be created which usually sends out a notification mail to the administrator. ▪ **Send report by email only**: Create a PDF file of the report and send it via email once it is finished. The report is not permanently stored, but only emailed. Define an email address below.
Email Address	This setting is only visible if a send by email option is selected above. Please enter a valid email address the report will be sent to. To enter more addresses, separate them by comma. Email configuration can be changed in the System Administration—Notification Delivery 877 settings.

Period	
Reported Period	Define the time span covered by the report. Choose between: ▪ **Current**: Use monitoring data of the current period. Define the period type below. ▪ **Previous**: Use monitoring data of the last period. Define the period type below.
Report Period Type	Define the type of period you want to create a report for. Choose between: ▪ **Day** ▪ **Week** ▪ **Month** ▪ **Year** Depending on your selection, different period selections are shown below.
Day Period	This setting is only visible if day period type is selected above. Define the hours when a day starts and ends. Choose from the list of hours. Default setting is **0:00-23:59**.
Week Period	This setting is only visible if week period type is selected above. Define when a week starts and ends. Choose between: ▪ **Monday-Sunday**: A reported week will start on Monday. ▪ **Saturday-Friday**: A reported week will start on Saturday. ▪ **Sunday-Saturday**: A reported week will start on Sunday.
Month Period	This setting is only visible if month period type is selected above. Define when a month starts and ends. Choose between: ▪ **1.-last day**: A reported month will start on the first and end on last of the month. ▪ **15.-14.**: A reported month will start von 15th and end on 14th of the month.

© 2011 Paessler AG

Period	
Year Period	This setting is only visible if year period type is selected above. Define when a year starts and ends. Choose between: ▪ **1/1-12/31**: A reported year will start on January 1st. ▪ **7/1-6/30**: A reported year will start on July 1st.
Report only for specific hours-of-day (Schedule)	Include certain time spans within the defined period only. When a schedule is selected, only monitoring data for specified hours or weekdays within the defined period are included in the report. Select **None** to include all available monitoring data in the report, or choose a schedule. For example, select the schedule **Weekdays** to exclude all weekends from the report. The available schedules depend on your configuration. For more information, please see Account Settings—Schedules 868 section.

Percentile Settings	
Show Percentile	Define if percentiles will be included in the report. Choose between: ▪ **Off**: Do not show percentiles ▪ **On**: Add a column to data tables, showing percentiles for every sensor channel. *Note:* Percentiles are not available for all report templates. If a template does not support percentiles, they will simply not show up in the report, even when you enable this setting.

Report Comments	
Introduction	Define a custom text that will show up on the first page of the report. Please enter a string or leave the field empty.
Footer Comments	Define a custom text that will show up on the last page of the report. Please enter a string or leave the field empty.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists. • **Read**: Users in this group can see the object and review its settings. • **Write**: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. • **Full**: Users in this group can see the object, as well as review and edit its settings and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Select Sensors Manually

Click on the **Select Sensors Manually** tab to manually choose sensors that will be included in the report. The page for this tab is split into two areas: In the upper area, you see your selection of all manually added objects. In the lower area, you can navigate to objects you want to add. You can perform the following actions:

- **Add**
  In the lower area, click on the **Add** link at the end of a line to include an object. It will be added to the upper area, which shows your selection. If you add a probe, group, or device to your selection, all sensors on this object will be included in the report.

- **Navigate**
  In order to find objects in the lower area, use the **Search** field to filter objects, or navigate through the list 119.

- **Delete**
  In the upper area, click on the **Delete** link at the end of a line to remove an object from the selection.

- **Sensor Channel Selection**
  If in the report settings one specific cluster node is selected *and* if you are adding a sensor to the selection, you can specify the sensor channels that will be included in the report. By default, all channels are selected. To exclude a channel from the report, simply remove the check mark in front of a channel's name. *Note:* If **All nodes** is selected in the report's **Cluster Node** selection, the channel selection is not available, but only the primary channel of every sensor is included automatically.

Your selection is saved automatically, and there is no undo function. *Note:* The final report will include both sensors selected manually and those selected by tag.

Sensors Selected by Tag

Click on the **Sensors Selected by Tag** tab to view all sensors that are added to the report depending on the report's **Add Sensors by Tag** setting. In the table list 119, you will see all sensors that are added by tag. This is for your information only, you cannot change sensors here. However, you can switch to the report's **Settings** tab and change the tabs that are used to add sensors. Additionally, you can also exclude sensors with certain tabs there. The final report will include both sensors selected manually and those selected by tag.

For sensors that are added by tag, all sensor channels are included in the report automatically, except **All nodes** is selected in the report's **Cluster Node** selection. In this case, only the primary channel of every sensor is included. *Note:* The final report will include both sensors selected manually and those selected by tag.

© 2011 Paessler AG

Comments

In the **Comments** tab you can enter free text for each object. This can be used for documentation purposes or to leave information for other users.

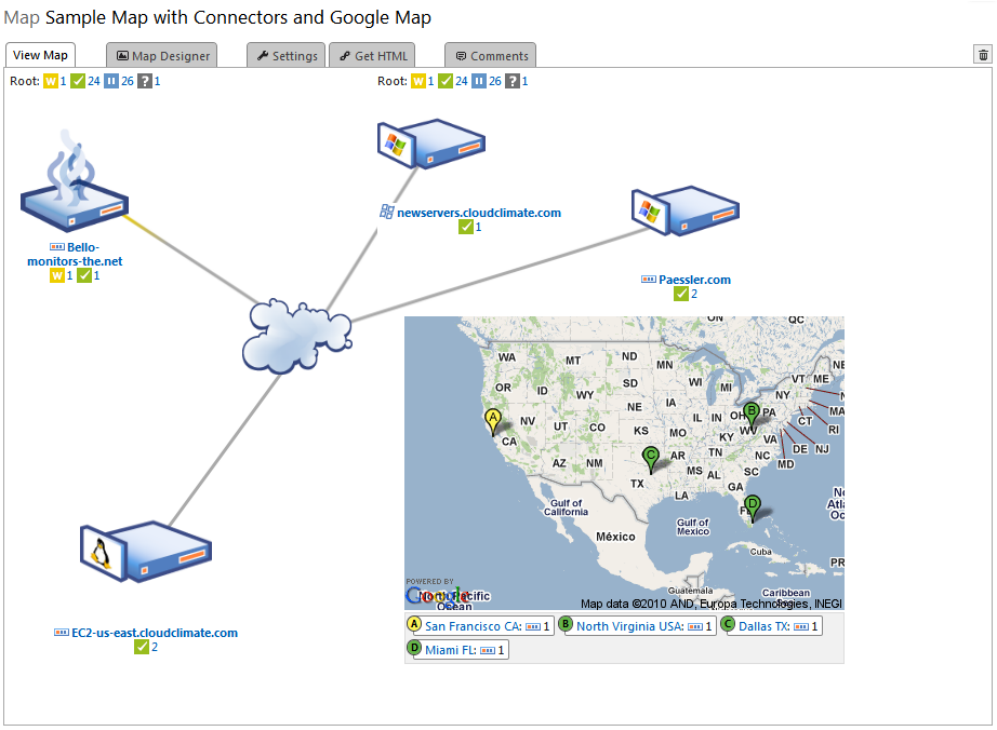
More

Knowledge Base: How do I modify PRTG's report templates?

- http://www.paessler.com/knowledgebase/en/topic/263
- **Calculating Percentiles** 995

7.11 Maps

With PRTG's **Maps** feature (some people might call this 'dashboards') you can create web pages with up-to-the-minute monitoring status information in a customizable layout. Using this unique concept, you can also make your overview pages of live data publicly available, if you like.



Example of a PRTG Map

In this section:

- Introduction 842
- Start Maps 843
- Maps Overview 843
- Maps Rotation 844
- Working with Maps 844

Introduction

There are countless possibilities for the implementation of maps. For example, this feature can be used to:

- Create network maps with status icons for each device on the map.
- Create quick views of your network that can be shown on network operations center screens.
- Create a quick network overview for publishing on the Intranet, allowing at-a-glance information for management of other employees.
- Create a custom view of the most important sensors in your monitoring setup.
- Create Top 10 lists of the sensors of a specific group or device.

© 2011 Paessler AG

Technically, a map is a usual HTML web page. You can build a schema of your network by choosing from hundreds of device icons and connect them with lines. A map can consist of the following elements:

- A set of map items, which can include device icons, sensor status icons, graphs, data tables, lists of sensors, connection lines, geographical maps, or custom HTML code.
- An optional background image (a JPG, PNG, or GIF file, e.g. your company logo or a graphical view of your network).

You can also specify the size of the map. Using the AJAX-based map editor, you can place the items anywhere on the map and you can also change their size. Each map has a unique URL which can be used to link to the map. Users who want to access the map either need an account in your PRTG installation, or can access a public URL of the map if you allow the **Public Access** feature. Public maps contain a unique **Map ID** access key in the URL to block unwanted visitors.

Start Maps

Click the **Maps** entry from the main menu 137 to view or add custom views of your network's status and monitoring data. *Hover* to show other menu items. Choose between:

- **All**
  Calls the Maps feature where you can view or add custom views of your network's status and monitoring data.

- **Add Map**
  Lets you directly add 845 a new map.

- **Select Map ›**
  Show existing maps. *Hover* to show other menu items. Follow the menu path (it is specific to your setup) to select a map.

Maps Overview

In the **All** view, you see a list of all existing maps. Using the links next to a map name, you can perform the following actions.

- Click on the name of a map to view it.

- **Delete**: Delete this map.

- **Clone**: Create an exact copy of this map. As soon as you click, the map is cloned and the cloned map's settings are shown.

- Click on the **Add Map** button to add a new map.

Please see also **Working with Table Lists** 119. Additionally, there is multi-edit available. This enables you to change properties of several objects at a time. For more details, please see **Multi-Edit Lists** 813 section.

Map Rotation

To show several maps in a rotation, mark the desired maps using multi-edit 813 and then select **Map Rotation** from the multi-edit menu.

While a map rotation is shown, you can change the refresh interval any time when hovering the arrows symbol in the lower right corner. Choose between **10**, **30**, or **60** seconds, **10** minutes or **Refresh** now.

Working with Maps

For detailed information on how to create and edit maps, and to learn how to make them accessible to others, please see the following sections.

- Maps Step By Step 845
- Maps Designer 847
- Maps Other Settings 854

© 2011 Paessler AG

7.11.1 Maps Step By Step

In order to create a new map, follow the steps in this section. In the web interface, click on **Maps** entry in the main menu to show the maps main screen.

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

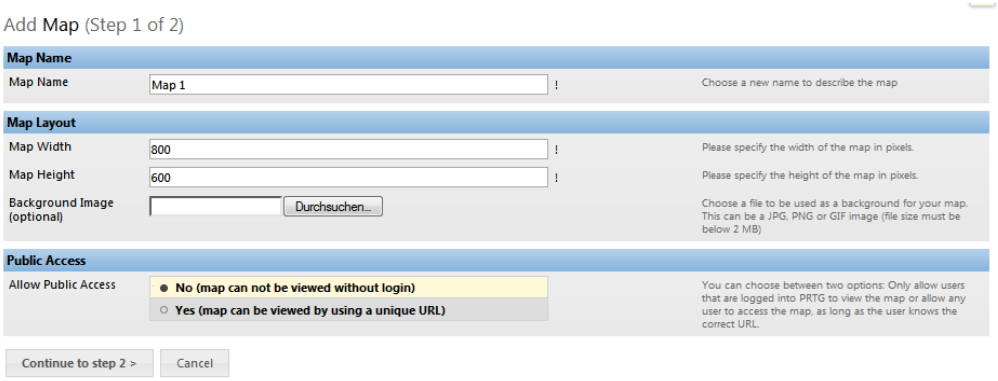
In this section:

- Step 1: Add Map 845
- Step 2: Add Map Items 845
- Step 3: View and Share 846

Step 1: Add Map

Click on the **Add Map** button. An assistant is shown. Enter a **Map Name** and define **Map Layout** settings. in the **Public Access** section, define whether your map will be visible without login.

For detailed information, see Maps Other Settings 854 section (Settings).


Add Map (Step 1 of 2)
Map Name
Map Name
Map 1
Choose a new name to describe the map
Map Layout
Map Width
800
Please specify the width of the map in pixels.
Map Height
600
Please specify the height of the map in pixels.
Background Image (optional)
Durchsuchen...
Choose a file to be used as a background for your map. This can be a JPG, PNG or GIF image (file size must be below 2 MB)
Public Access
Allow Public Access
No (map can not be viewed without login)
Yes (map can be viewed by using a unique URL)
You can choose between two options: Only allow users that are logged into PRTG to view the map or allow any user to access the map, as long as the user knows the correct URL.
Continue to step 2 >
Cancel

Add Map Assistent Step 1

Step 2: Add Map Items

Click on the **Add Map Item** button to open the **Add Map Object** assistant. Select an object, define further settings and confirm. The item will be added immediately. Repeat this procedure as often as you wish until you have added all desired items to the map. Drag items to change their position. Additionally, you can also draw connection lines between items or edit existing items.

For detailed information, see Maps Designer 847 section.

Step 3: View and Share

Click on the **View Map** tab to see the appearance of your map. Later, It will be shown the way you see it there. If available for an object, most object names as well as all sensors can be clicked on. It depends on the object's access rights and the currently logged in user account if clicking the links will lead to more detailed information about the object or to an error message indicating insufficient access rights.

Click on the **Get HTML** tab to get the direct URL of your map that you can share with others. For detailed information, see Maps Other Settings 856 section (Get HTML).

© 2011 Paessler AG

7.11.2 Maps Designer

Note: This section refers to PRTG Network Monitor version **8.4**. The Map Designer was significantly enhanced with this version. If you're using an earlier version, please update 37 to the latest version to profit from the innovations.

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

In this section:

- Use a Proper Browser 847
- Basic Design Concept 847
- Device Tree Selection 848
- Properties Selection 849
- Edit Existing Map Items—Properties Box 850
- Edit Existing Map Items—Hover Icons 851
- Edit Existing Map Items—Using Cursor Keys 851
- Draw Connection Lines Between Items 851
- Snap To Grid 852
- More 852

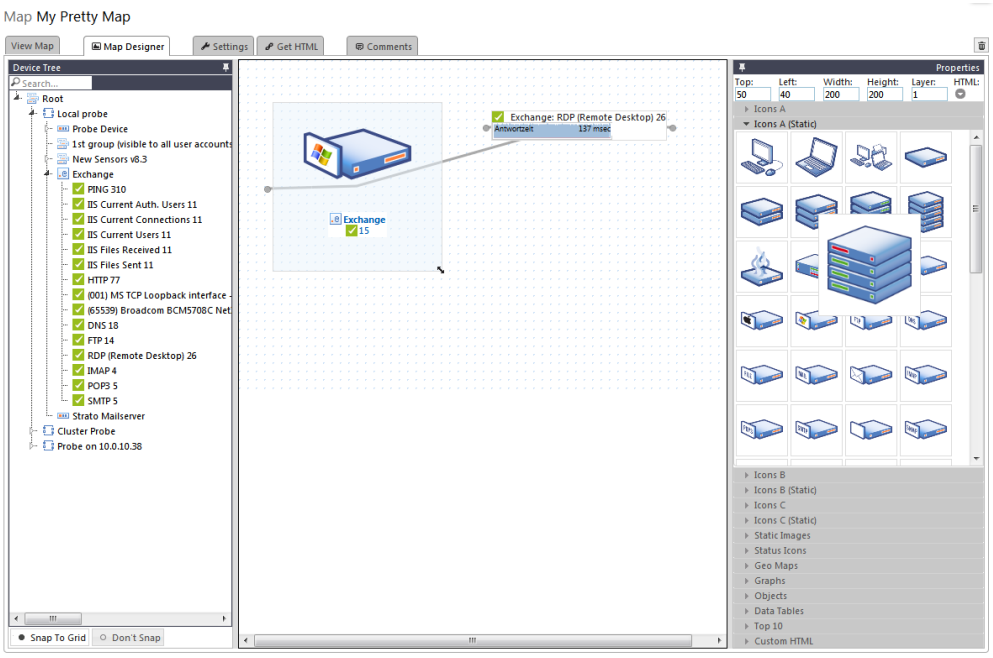
Click on the **Go to all maps** button at the bottom of the page to return to the list of Maps.

Use a Proper Browser

Due to the map designer's extensive scripting capability, it is important that you use a compatible browser when editing maps. We recommend using Mozilla Firefox 3 or 4, or Google Chrome. You can use Internet Explorer 9 as well. The maps designer is *not* fully compatible with earlier versions of Internet Explorer or Opera browsers.

Basic Design Concept

Click on the **Map Designer** tab to open the editor. It might take a few moments to load (for *unresponsive script* warnings, please see More 852 section below). Here, you can create your map by adding or changing items. The designer screen consists of three main parts: The **Device Tree** on the left side, the current **Map** in the middle, and the **Properties** on the right side.



Map Designer

Each map item takes attributes from both selections.

- **Device Tree** (left): Select the monitoring object which's data will be shown on the map
- **Properties** (right): Define how the map item will be shown

Simply drag and drop any object from either side onto the map, or double-click on an object. You will always see all changes immediately.

Device Tree Selection

Use the **Device Tree** to select the monitoring object which's data will be shown on the map (this can be a probe, a group, a device, or a single sensor). In order to find the right object, you have the following options:

- Use the arrow symbols at the beginning of each line to open nodes in the device tree to show objects underneath probes, groups, and devices.

- Enter a view characters into the **Search** box in the upper left corner to search for names (or part of names) of objects in your configuration. The search results will be shown immediately. Click on the red **x** icon to clear your search.

No matter which method you choose to find the desired object, you can always drag any object from the **Device Tree** on a free area of the map to create a new map item. If you drag it onto an existing map item, it will be replaced, while **Properties** and size will remain. You can also select a map item and double click on a **Device Tree** object to replace the map item. If no item is selected, a double-click on an object will add a new map item.

© 2011 Paessler AG

To gain more space for map editing, click on the pin symbol in the upper right corner of the **Device Tree** box to swing it in. Click it a second time to fix the box again. You can also resize the box by dragging its right border to left or to the right

Properties Selection

Use the **Properties** selection to define how the map item will be shown (for example, as an icon, a map, a table, or a graph). Select the appearance in different categories. Hover a property object to get a live preview of it (in most cases). *Note:* If a certain **Properties** object is not available for the selected **Device Tree** object, you will see a corresponding text hint.

There are many different property object types available. Simply click a category's name to show all available types.

- **Icons A, Icons B, Icons C**
  These three categories offer a variety of iconic symbols of typical network devices. Below each icon the object name and a sensor overview for the object is shown. This shows how many sensors are in which state. For some sensors, a mini graph is shown as well.
- **Icons A (Static), Icons B (Static), Icons C (Static)**
  These three categories offer the same variety of iconic symbols of typical network devices as the category described above. Here, no object data displayed with them, but only the icon is shown.
- **Static Maps**
  This category offers free or public domain geographical maps from different sources. For additional geographical maps, please see More 852 section below. *Note:* The items in this section are independent from the selected **Device Tree** objects.
- **Status Icons**
  This category shows options to insert status icons in different styles. These show the object name and an overview of how many sensors are in which state. There is also an object available for audible alert which will play a sound when the number of alarms of the monitored object are > 0. Please note that your browser must support playing embedded sounds (see More 852 section below for further information).
- **Geo Maps**
  In this category you can choose from different geographical map styles from Google: road map, satellite, hybrid, and terrain maps. The location of the currently selected object in the **Device Tree** will be shown on the map as a pin mark. To use this feature, Geo Maps integration must be enabled and you have to enter a **Location** in the settings of the monitoring object you want to use this with. For more information, please see Geo Maps 823 section. *Note:* If Geo Maps integration is disabled, you will only see white boxes instead of map previews.
- **Graphs**
  This category offers different graph styles in several dimensions and detail. You can also select graphs including a legend or sensor states.
- **Objects**
  Add some simple geometric shapes to your map. The items shown in this tab are always the same; the range displayed does not depend on the selected object in the **Object** field above.

© 2011 Paessler AG

- **Data Tables**
  Choose from several tables showing sensor lists for the current selected object. You can also choose from several lists showing sensors in a certain state only.

- **Top 10**
  Choose from several tables showing the top 10 of sensors with certain monitoring data, such as least used CPUs, highes bandwidth usage, best availability, slowest websites, etc. *Note:* In order to provide live previews, PRTG calculates all top 10 lists from your monitoring data when opening this tab. It may take a few seconds before thumbnails are shown.

- **Custom HTML**
  This can be used, for example, to add external images or applets to your map. In order to actually add custom HTML code to your map, please add this item and then click on it to edit 850. You can then copy your custom code into the **HTML Before** and **HTML After** fields in the **Properties** box on the right side.

No matter which object you choose, you can always drag any object from the **Properties** box on a free area of the map to create a new map item. If you drag it onto an existing map item, it will be replaced, while its **Device Tree** object attributes and size will remain. You can also select a map item and double click on an object in the **Properties** box to replace the map item. If no item is selected, a double-click on an object will add a new map item.

To gain more space for map editing, click on the pin symbol in the upper right corner of the **Properties** box to swing it in. Click it a second time to fix the box again. You can also resize the box by dragging its left border to left or to the right.

Edit Existing Map Items—Properties Box

Click on a map item to select it. You can then edit its attributes with the fields in the upper part of the **Properties** box on the right side:

- **Top**, **Left**, **Width**, and **Height** fields
  Enter position and size values for direct positioning. Click the **Save** button to save your settings. Alternative: Use the mouse to move and resize a map item.

- **Layer** field
  The layer number defines if an item will be shown on top of or behind another item, if overlapping. The item with the higher number will be shown on top. Enter a positive integer value and click the **Save** button to save your settings. Alternative: Use the arrow symbols in a map item's hover menu to **Bring to front** or **Send to back** an item one layer (see below).

- **HTML**
  Click on the arrow symbol underneath to show the **HTML Before** and **HTML After** fields. Any HTML code you enter in these fields will be added before respectively after the map item. Please enter your custom HTML code that embeds an objects and click the **Save** button. Your HTML object will be inserted. For example, you could enter the code *<img src="http://media.paessler.com/common/img/logoclaim_r1.gif">* to insert an image of the Paessler logo from the Paessler website.

© 2011 Paessler AG

Edit Existing Map Items—Hover Icons

Hover a map item to show the edit icons for it.

Edit Icons of a Maps Object

- **Bring to front (arrow up symbol)**
  Move this item one layer to the front. This is useful when adding several items to a map that overlap each other.

- **Send to back (arrow down symbol)**
  Move this item one layer to the back. This is useful when adding several items to a map that overlap each other.

- **Delete (trash symbol)**
  Delete this item. *Note:* Be careful! The item will be deleted immediately without notice and you cannot undo this. Alternative: Select the item and press the *Del* button on your keyboard.

- **Drop Connections (scissors symbol)**
  If you have drawn connection lines between two items, you can delete all lines starting from this item. Connection lines will be dropped immediately. *Note:* If a line between two items is not dropped, you've probably drawn it starting from the other item. Try the scissors symbol on the other item instead.

Edit Existing Map Items—Using Cursor Keys

While an object is selected, use the cursor keys to move it by one pixel. Hold the *Shift* key in combination with the cursor keys to move the object by 10 pixels.

Draw Connection Lines Between Items

You can draw connection lines between any map items via drag and drop. Simply click on the grey handles next to an item and drag a line to another item you want to draw a connection to. A line will be shown immediately. This can be useful to indicate network connections or logical coherences between two items. To delete connection lines, click the scissors symbol in the item's edit icons 850.

Icons with Colored Lines

For objects with a graphical icon, dynamical line coloring is active. If you draw a line from such an object, it will turn red as long as one of the object's icons shows a red **Down** status. This will only affect half of the line, at the end where the red sensor is shown. If both objects connected show a red sensor, this will result in a line that is red all over. *Note:* Currently, this feature is unavailable for objects that do not show a graphical icon. For example, this concerns status icon objects, geographical maps, graphs, data tables, and top lists. Lines will always remain grey at the end of these objects.

Snap to Grid

Select whether to use **Snap To Grid** or **Don't Snap**, using the buttons underneath the **Device Tree** box. This will affect how map items will be positioned when adding or moving them via drag and drop. The setting is active immediately. With snap to grid enabled, you can place items aligned with the grid only.

More

Knowledge Base: Why does my browser show an unresponsive script warning while loading the Maps Designer?
- http://www.paessler.com/knowledgebase/en/topic/19483

Knowledge Base: Where can I download free political/topographical map images for use in PRTG 8 map editor?
- http://www.paessler.com/knowledgebase/en/topic/7463

Knowledge Base: How can I setup audible notifications (sound files) in PRTG?
- http://www.paessler.com/knowledgebase/en/topic/5473

Knowledge Base: How can I add "deep links" into PRTG's interface for map status icons?
- http://www.paessler.com/knowledgebase/en/topic/3763

Knowledge Base: How can I add or edit map objects used for PRTG's maps?
- http://www.paessler.com/knowledgebase/en/topic/1703

Knowledge Base: How to setup interactive maps?
- http://www.paessler.com/knowledgebase/en/topic/2253

Knowledge Base: Can you re-order or remove columns in sensor lists displayed in maps?
- http://www.paessler.com/knowledgebase/en/topic/5523

Knowledge Base: How can I show up-to-date weather information, webcam and radar images in PRTG's maps

© 2011 Paessler AG

- http://www.paessler.com/knowledgebase/en/topic/9263

Knowledge Base: Can I use my own images/icons/logos in PRTG's map editor?

- http://www.paessler.com/knowledgebase/en/topic/8043

7.11.3 Maps Settings

Using the Map tabs you can access all functionalities and settings for a map.

Maps Tabs

Click on the **Go to all maps** button at the bottom of the page to return to the list of Maps.

View Map

Click on the **View Map** tab any time to show a preview of your map.

Map Designer

Click on the Map Designer tab to edit the contents of your map. Please see Maps Designer 847 section.

Settings

Click on the **Settings** tab to open a map's general settings. *Note:* When using the **Add Map** dialog, not all of these settings are available. You can change them later by clicking on the **Settings** tab.

Basic Map Settings	
Map Name	Enter a meaningful name for the map.
Security Context	Define the user account that will be used for access to monitoring data. The map will only contain objects which the selected user 89 is allowed to view. Please choose a user from the list. The available users depend on your configuration. By default, this is the user that created the map. PRTG Administrator users can change this setting.
Timezone	Define the time zone that will be used for all date-specific options in this map. Select a time zone from the list.
Tag Filter	This setting affects table maps objects. Enter one or more tags separated by space or comma to include sensors in tables. Only sensors with one of the tags entered here (including inherited tags from parent objects) will be appear in this map's data tables. Please enter a string or leave the field empty.

Map Layout	
Map Width	Define the width of the map in pixels. Please enter an integer value.
Map Height	Define the height of the map in pixels. Please enter an integer value.
Background Picture	Define if you want to use a background picture for the map. Choose between:

© 2011 Paessler AG

Map Layout	
	▪ **On**: Use a background image (define below). ▪ **Off**: Do not use a background image.
Background Image	This option is only visible if a background picture is enabled above. Click on the **Choose File** button and select an image from your computer or network. *Note:* Only images in the format JPG, PNG, and GIF are supported. The image must be smaller than 18 MB. If you try to upload other images, you will get an error message. In a cluster, background images are not automatically deployed to the other nodes! In order to view maps on other nodes, please copy the background pictures manually to *\website\mapbackground* of the program directory on every node. For detailed information on how to find this path, please see More 856 section below.

Public Access	
Allow Public Access	Define if others can see the map. Choose between: ▪ **No (map can not be viewed without login)**: Do not allow public access to the map. Only users with both a login to the PRTG web interface and sufficient access rights can see the map. ▪ **Yes (map can be viewed by using a unique URL)**: Allow access to the map using a unique address. The URL contains an ID that you can change below.
Map ID	This field is only visible if public access is enabled above. An ID is automatically generated. It is part of the public URL for the map. We recommend using the default value. For more information on public access, please see the Get HTML 856 section.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists. • **Read**: Users in this group can see the object and review its settings. • **Write**: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. • **Full**: Users in this group can see the object, as well as review and edit its settings and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Get HTML

Your PRTG map is like a standalone HTML page. You can make it accessible to others, if you like. Depending on the **Public Access** setting 854 of your map, a visitor will need to provide PRTG user account login data to view the map, or will see the map immediately using a URL containing a unique ID. When using the unique ID, you can also include your map on another webpage, embedding it via *<iframe>*.

- **Option 1: Link to a web page with the map**
  Two URLs are shown: One for access with login, and another for direct access without login. In order for the URL without login to work, you must enable **Public Access** in the settings tab 854 of your map. *Note:* In the URL, manually replace the string **YOUR_PRTG_SERVER_IP** by the IP address or DNS name via which the page is available. PRTG cannot determine this automatically, as there may be a NAT translation set in your firewall, or you may want to use a domain name or a name from a dynamic DNS service for public access.

- **Option 2: Show a map inside other web pages using an IFRAME**
  For your convenience, this shows source code for adding an iframe to another webpage. It includes a URL for direct access. Just copy the code and paste it into your webpage's code. *Note:* In the URL, manually replace the string **YOUR_PRTG_SERVER_IP** by the IP address or DNS name via which the page is available. PRTG cannot determine this automatically, as there may be a NAT translation set in your firewall, or you may want to use a domain name or a name from a dynamic DNS service for public access.

While a map is shown via these URLs, you can change the refresh interval any time by hovering the arrows symbol in the lower right corner. Choose between **10**, **30**, or **60** seconds, **10** minutes or **Refresh** now.

Comments

In the **Comments** tab you can enter free text for each object. This can be used for documentation purposes or to leave information for other users.

Delete

You can delete the entire map any time by clicking on the trash symbol on the right.

More

Knowledge Base: How and where does PRTG store its data?
- http://www.paessler.com/knowledgebase/en/topic/463

Knowledge Base: How to disable links in public maps?
- http://www.paessler.com/knowledgebase/en/topic/10283

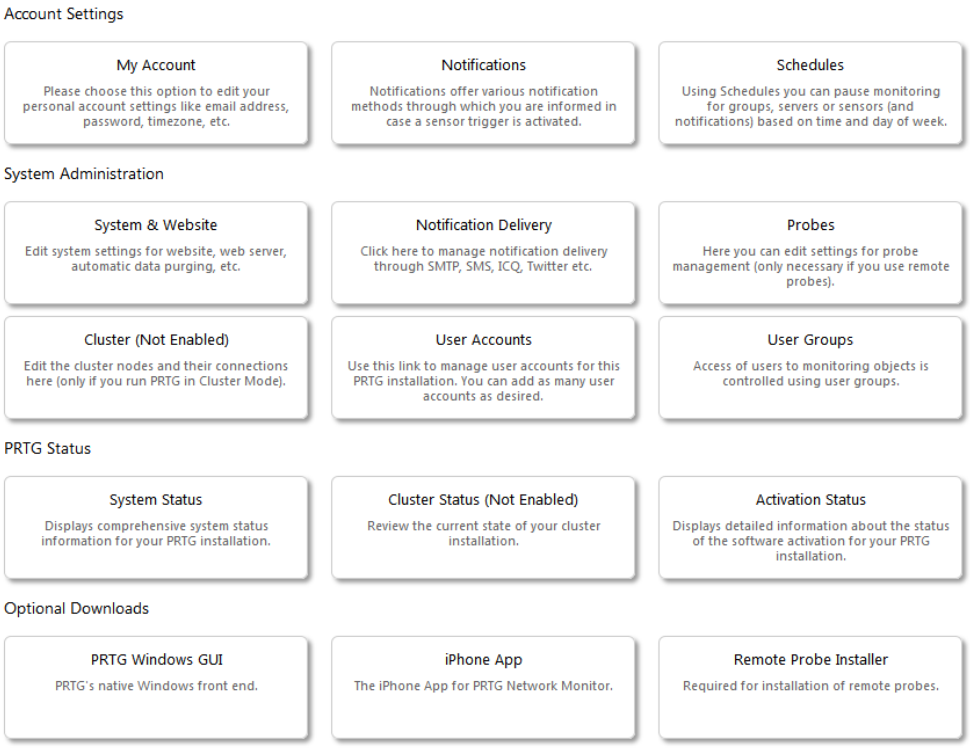
- **Data Reporting** 88

© 2011 Paessler AG

7.12 Setup

In the setup settings of the PRTG web interface, you can define almost all system settings for PRTG. However, some of the machine-oriented settings are defined using two Windows administration programs (see Others 858 section below).

In the main menu, click on **Setup** to show the available options.


Account Settings
My Account
Please choose this option to edit your personal account settings like email address, password, timezone, etc.
Notifications
Notifications offer various notification methods through which you are informed in case a sensor trigger is activated.
Schedules
Using Schedules you can pause monitoring for groups, servers or sensors (and notifications) based on time and day of week.
System Administration
System & Website
Edit system settings for website, web server, automatic data purging, etc.
Notification Delivery
Click here to manage notification delivery through SMTP, SMS, ICQ, Twitter etc.
Probes
Here you can edit settings for probe management (only necessary if you use remote probes).
Cluster (Not Enabled)
Edit the cluster nodes and their connections here (only if you run PRTG in Cluster Mode).
User Accounts
Use this link to manage user accounts for this PRTG installation. You can add as many user accounts as desired.
User Groups
Access of users to monitoring objects is controlled using user groups.
PRTG Status
System Status
Displays comprehensive system status information for your PRTG installation.
Cluster Status (Not Enabled)
Review the current state of your cluster installation.
Activation Status
Displays detailed information about the status of the software activation for your PRTG installation.
Optional Downloads
PRTG Windows GUI
PRTG's native Windows front end.
iPhone App
The iPhone App for PRTG Network Monitor.
Remote Probe Installer
Required for installation of remote probes.

Setup Overview

Account Settings

- Account Settings—My Account 859
- Account Settings—Schedules 868
- Account Settings—Notifications 862

System Administration

- System Administration—System and Website 871
- System Administration—Notification Delivery 877
- System Administration—Probes 881
- System Administration—Cluster 883
- System Administration—User Accounts 884
- System Administration—User Groups 887

PRTG Status

- PRTG Status—System Status 888
- PRTG Status—Cluster Status 888
- PRTG Status—Activation Status 889

Optional Downloads

- Downloads 890

Others

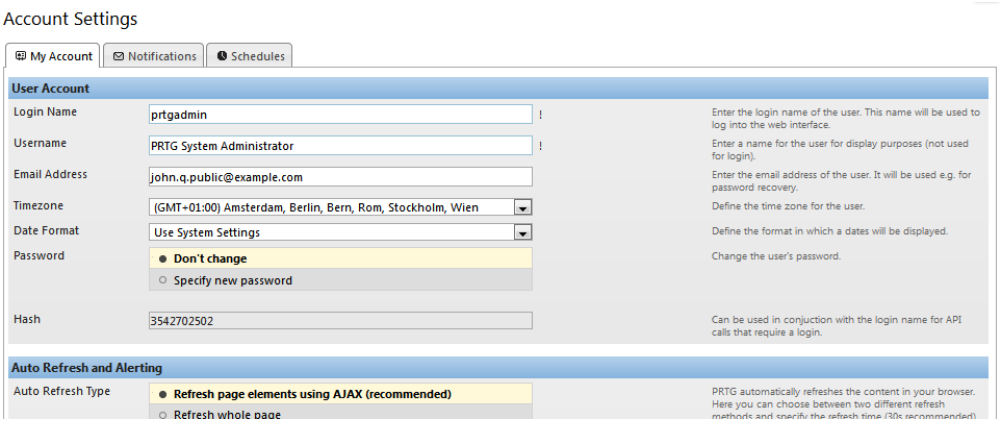
There are some settings that have to be made in the system administration programs 954, running as Windows applications. For more details, please see sections:

- PRTG Server Administrator 955
- PRTG Probe Administrator 969

© 2011 Paessler AG

7.12.1 Account Settings—My Account

In the my account settings you can define values regarding your own PRTG user currently logged in. All settings in this section are user specific. Some account control options may not available, but can only be defined by the administrator.


Account Settings
My Account
Notifications
Schedules
User Account
Login Name
prtgadmin
Enter the login name of the user. This name will be used to log into the web interface.
Username
PRTG System Administrator
Enter a name for the user for display purposes (not used for login).
Email Address
john.q.public@example.com
Enter the email address of the user. It will be used e.g. for password recovery.
Timezone
(GMT+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
Define the time zone for the user.
Date Format
Use System Settings
Define the format in which a dates will be displayed.
Password
Don't change
Specify new password
Change the user's password.
Hash
3542702502
Can be used in conjuction with the login name for API calls that require a login.
Auto Refresh and Alerting
Auto Refresh Type
Refresh page elements using AJAX (recommended)
Refresh whole page
PRTG automatically refreshes the content in your browser. Here you can choose between two different refresh
My Account Settings

My Account Settings

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

User Account	
Login Name	Enter the login name for the user.
Username	Enter a name for the user for display purposes. This will not be used for login.
Email Address	Enter the user's email address.
Timezone	Enter the time zone for the current user.
Date Format	Enter in what format dates will be displayed for the current user.
Password	Define the user's password. For security reasons, the account settings page does not contain the password. Choose between: ▪ **Don't change** ▪ **Specify new password** If you choose to specify a new password, enter the old password, and the new password twice.
Hash	The hash (passhash) value can the used as password substitute when calling functions from PRTG's Application Programming Interface (API) that require an authentication. For more information please see Using the PRTG API (Application Programming Interface) 979 section.

Auto Refresh and Alerting	
Auto Refresh Type	Specify how PRTG's web pages will be refreshed for the current user. Choose between: ▪ **Refresh page elements using AJAX (recommended)**: Automatically refresh the single page elements on the web pages. ▪ **Refresh whole page**: Automatically reload the whole page with every refresh interval. ▪ **No auto refresh**: Do not automatically refresh web pages.
Auto Refresh Interval (sec)	This setting is only relevant when auto refresh is enabled above. Enter the number of seconds that will be waited between two refreshes. We recommend using **30** seconds or more. Minimum value is 20 seconds. *Note:* Shorter intervals create more CPU load on the server running the PRTG core server. If you experience load problems while using the web interface (or PRTG maps 842), please set a higher interval.
Play Audible Alarms	Define when an audible alarm will be played for the current user on web pages whenever there are alarms 113 in PRTG. Choose between: ▪ **Never**: Do not play sound files on any web pages. ▪ **On dashboard pages only**: When there are alarms, play a predefined sound on dashboard 133 pages only. The sound will be replayed with every refresh of a dashboard page. ▪ **On all pages**: When there are alarms, play a predefined sound on all web pages. The sound will be replayed with every page refresh. For more information about audible notifications and supported browsers, please see **More** 861 section below.

Web Interface	
Homepage URL	Define the user's default page loaded after login and when clicking on the Home 133 button in main menu.
Max. Groups/Devices per Group	In order to provide you with a speedy user experience PRTG tries to keep the page size for the page showing sensor trees small by automatically folding groups and devices with many items. Define how many groups and devices are shown at maximum before the automatic reduction is performed. We recommend using a value between **10** and **30**.
Max. Sensors per Device	In order to provide you with a speedy user experience PRTG tries to keep the page size for the page showing sensor trees small by automatically folding groups and devices with many items. Define how many sensors are shown at maximum before the automatic reduction is performed. We recommend using a value between **10** and **30**.

Account Control	
Account Type	This setting is only shown for administrator users. Define the account type for the current user. Choose between: ▪ **Read/Write User**: The user may change settings.

© 2011 Paessler AG

Account Control	
	▪ **Read Only User**: The user may not edit any settings. This is a good choice for public or semi-public logins. *Note:* This setting cannot be changed for the default administrator user.
Primary Group	This setting is only shown for administrator users. Select the primary group for the current user. Every user has to be member of a primary group to make sure there is no user without group membership. Membership in other user groups is optional. For user experience, there is no difference between the primary and other user groups.
Status	This setting is only shown for administrator users. Define the status of the current user. Choose between: ▪ **Active**: The current user can login to the account. ▪ **Inactive**: The current user's login is disabled. Use this option to temporarily deny access for this user. *Note:* This setting cannot be changed for the default administrator user.
Last Login	Shows the time stamp of the user's last login. This setting is shown for your information only and cannot be changed here.

User Groups	
Member of	Shows the groups the current user is member of. Access rights to the device tree are defined on group level. This setting is shown for your information only and cannot be changed here.

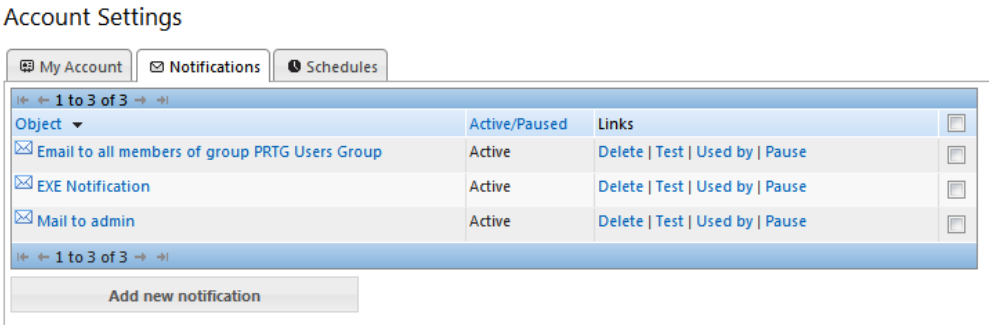
Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: How can I setup audible notifications (sound files) in PRTG?
- http://www.paessler.com/knowledgebase/en/topic/5473

7.12.2 Account Settings—Notifications

In the notifications settings you can define and change notifications for the currently logged in PRTG user. They can be triggered for certain sensor states and data.



Notifications Settings

Note

This section describes one of three steps to set up the notification system in PRTG. A complete notification setup involves:

1. Defining notification delivery settings
2. Setting up notifications
3. Adding notification triggers to sensors

For more information please see Notifications 826 section.

Notifications Settings

Click on the **Notifications** tab to show a list of all existing notifications. Using the links next to the notification name, you can perform the following actions:

- **Delete**: Delete this notification (not possible for predefined notifications)
- **Test**: Trigger this notification immediately for testing purposes. *Note:* When using placeholders, they will not be resolved in a test notification, but the variables will be sent instead.
- **Used by**: Show a list of objects using this notification.
- **Pause**: Pause this notification. If a notification is paused, no messages will be sent when it is triggered.

Please see also Working with Table Lists 119. Additionally, there is multi-edit available. This enables you to change properties of several objects at a time. For more details, please see Multi-Edit Lists 813 section.

Click on the **Add new notification** button to add a new notification, or click on the name of an existing notification to edit it.

© 2011 Paessler AG

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Basic Notification Settings	
Notification Name	Enter a meaningful name for the notification, for example, *SMS to service team* or similar.
Status	Select the status of the notification. Choose between: ▪ **Started**: This notification will be active. ▪ **Paused**: Pause this notification. If a notification is paused, no messages will be sent when it is triggered.
Schedule	Define if this notification will be paused for certain time spans. Please select **None** to set it to always active, or choose a pausing schedule from the list. The available options depend on your setup. To add or change existing schedules, please see Account Settings—Schedules 868 section.
Postpone	Define if notifications triggered during **Pause** status will be sent later on. ▪ **No**: Discard all notification triggers received while the notification is paused. ▪ **Yes**: Collect all notification triggers received while the notification is paused. Send out notifications once the pause status ends.

Notification Summarization	
Method	Define if and how notifications will be summarized if several notification triggers are received in a certain time span. *Note:* Regardless of the option chosen here, notifications of **Execute HTTP Action** and **Execute Program** are always sent ASAP; they are never summarized. Choose between: ▪ **Always notify ASAP**: Always send out one notification for each notification trigger received. ▪ **Send first DOWN message ASAP, summarize others**: When receiving several **Down** triggers, send the first notification immediately, but summarize other notifications into one message. ▪ **Send first DOWN and UP message ASAP, summarize others**: When receiving several **Down** or **Up** triggers, send each first notification immediately, but summarize other notifications into one message. ▪ **Send all DOWN messages ASAP, summarize others**: When receiving several **Down** triggers, send out one notification for each trigger received, but summarize notifications for all other triggers into one message. ▪ **Send all DOWN and UP messages ASAP, summarize others**: When receiving several **Down** or **Up** triggers, send out one notification for each trigger received, but summarize notifications for all other triggers into one message. ▪ **Always summarize notifications**: When receiving several notification triggers, summarize all notifications into one message, regardless of the kind of trigger received.

Notification Summarization	
Gather Notifications For (Minutes)	Define a time span in minutes for which notifications will be collected for summarization. Please enter an integer value. *Note:* If you define a high value, for example, **60** minutes, PRTG will send out summarized notifications with a delay of up to one hour.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists. • **Read**: Users in this group can see the object and review its settings. • **Write**: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. • **Full**: Users in this group can see the object, as well as review and edit its settings and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings.

With the following settings, you can add one or more messaging options to the notification. Whenever the notification is triggered, it will send out a message or perform actions for all configured options. To add an option, add a check mark symbol in front of the respective setting name. You will then see the options described below.

Note: You can use various placeholders in your message. Some are already filled in by default. For a list of all placeholders, please see the More 826 section below.

Send Email	
Email Address	Enter one or more recipient email addresses. If entering more addresses, separate them by comma. If you want to send to a PRTG user group only, leave this field empty!
Address Group	From the list, choose a PRTG user group to which the email is to be sent.
Subject	Enter the subject of the email. Several placeholders (variables) are used here by default.
Format	Define the kind of email that will be sent. Choose between: ▪ **Text** ▪ **HTML**

© 2011 Paessler AG

Send Email	
Message	Depending on the format option selected above, you will see a text or HTML message in this field. A complete message about the sensor status is already predefined. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else). Click on the **Reset to default** link underneath the text box to do so.
Priority	Define the priority which will be set in the email. Some email clients can show this flag.

The email footer can be set in the system and website settings 871.

Add Entry to Event Log	
Logfile	Define the log file the message will be written to. Choose between: ▪ **Application**: Use the Windows application log file in the event log. ▪ **PRTG Network Monitor**: Write messages to the PRTG Network Monitor log file in the Windows event log.
Event Source	This setting is only relevant when using the **Application** log file. Enter the source for the event. Usually, this is the name of the application.
Event Type	Select the type of the event. Choose between: ▪ **Error** ▪ **Warning** ▪ **Information**
Event Log Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

Send Network Broadcast (NET SEND)	
User	Define the user or computer name of the receiver.
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

Note: NetSend is no longer supported on computers running Windows Vista, or later. Messages will be ignored on these systems.

Send Syslog Message	
Host/IP	Define the IP address or DNS name of the computer running the syslog server.

Send Syslog Message	
Port	Enter the port number on which syslog messages are sent. By default, this is port number **514**.
Facility	Define the facility information. There are several options available from the list.
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

Send SNMP Trap	
Host/IP	Define the IP address or DNS name of the computer running the trap receiver.
SNMP Port	Enter the port number on which trap messages are sent. By default, this is port number **162**.
Community String	Enter the device's community string. By default, this is set to **public**.
Message ID	This ID helps you indentify the origin of the trap. For example, enter *1.3.6.1.4.1.32446.1.1.1*
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).
Agent IP	Define the IP address of the agent. Leave this field blank to use the PRTG web server's IP address.

Send SMS/Pager Message	
Recipient Number	Define the number the message will be sent to. The format depends on the SMS provider. Usually, you will use a plus sign, followed by country code and number. For example, enter **+1555012345**.
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

Note: This notification method needs to be set up in the notification delivery settings 877 first.

Execute HTTP Action	
URL	Enter the URL the request will be sent to.

© 2011 Paessler AG

Execute HTTP Action	
Postdata	If you want to send postdata to the URL, please enter it here. You can use placeholders here.

Note: Regardless of the **Notification Summarization** method chosen above, notifications of **Execute HTTP Action** are always sent as soon as possible (ASAP); they are never summarized.

Execute Program	
Program file	Select an executable file from the list. It will be run every time the notification is triggered. In this list, files in the corresponding **/Notifications/EXE** sub-directory of the probe system's PRTG installation are shown. In order for the files to appear in this list, please store them as BAT, CMD, DLL, EXE, PS1, or VBS. *Note:* In a cluster setup, please copy your files to every cluster node installation manually. This makes sure the notification can be executed even when the master node fails. If your custom notification executes an external program, this has to be installed on all cluster nodes as well. Please see also Application Programming Interface (API) Definition 979 for detailed information.
Parameter	Enter parameters with which the program file will be started. You can use placeholders here. For example, when using a batch file containing a *%1* variable, you can provide a value for this variable here.

Note: Regardless of the **Notification Summarization** method chosen above, notifications of **Execute Program** are always sent as soon as possible (ASAP); they are never summarized.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

- Application Programming Interface (API) Definition 979

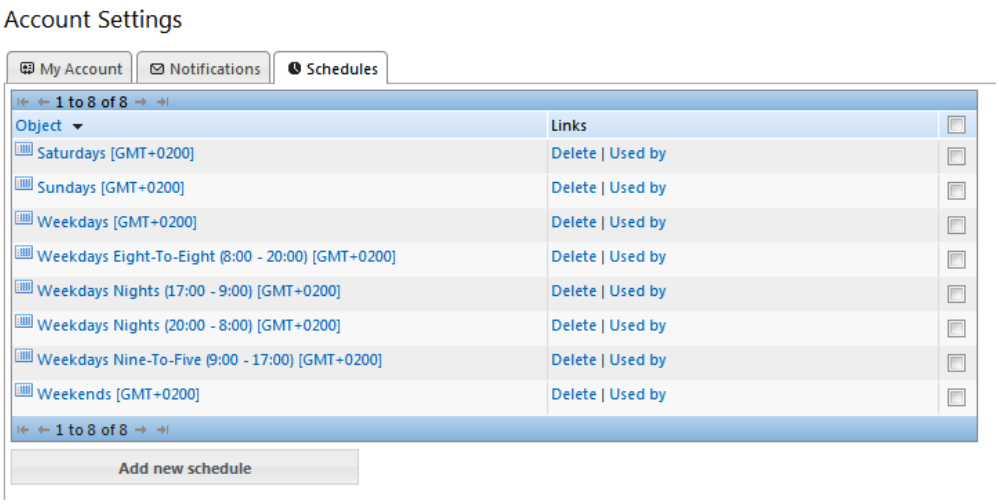
Knowledge Base: What placeholders can I use with PRTG?
- http://www.paessler.com/knowledgebase/en/topic/373

Knowledge Base: How and where does PRTG store its data?
- http://www.paessler.com/knowledgebase/en/topic/463

Knowledge Base: How can PRTG send instant messages to Jabber, ICQ, MSN, Yahoo, etc., using external software?
- http://www.paessler.com/knowledgebase/en/topic/14803

7.12.3 Account Settings—Schedules

In the schedules settings you can define and change schedules for the currently logged in user. This can be used to pause [123] monitoring at certain times. You can also use schedules to define the time spans that are to be covered when creating reports [827].



Schedules Settings

Schedules Settings

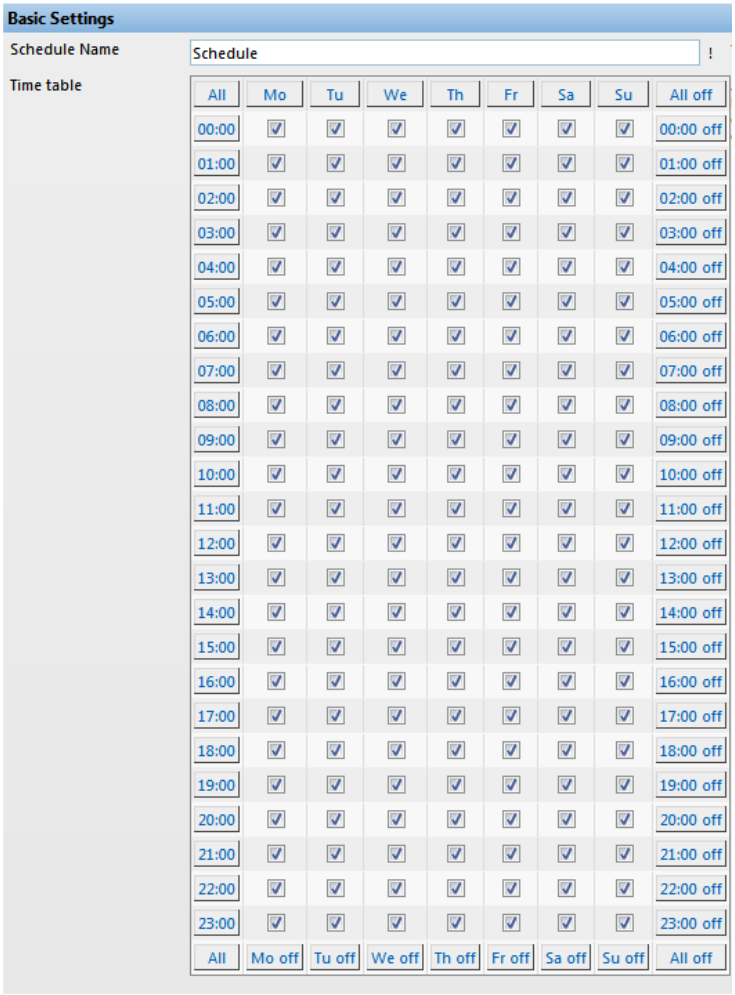
Click on the **Schedules** tab to show a list of all existing schedules. Using the links next to the notification name, you can perform the following actions:

- **Delete**: Delete this notification (not possible for predefined notifications)
- **Used by**: Show a list of objects using this notification.

Please see also **Working with Table Lists** [119]. Additionally, there is multi-edit available. This enables you to change properties of several objects at a time. For more details, please see **Multi-Edit Lists** [813] section.

Click on the **Add new schedule** button or click on the name of an existing notification to edit.

© 2011 Paessler AG



Edit Schedule Time Table

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Basic Settings	
Schedule Name	Enter a meaningful name for the schedule that describes the defined time span(s) or purpose.
Time Table	Define the schedule. It will be used for monitoring objects, reporting, and notifications. You can set time spans with a precision of one hour by setting check marks. If a box is checked, it means the object is active during this hour, if unchecked, the object will be paused during this hour. You can set check marks individually, or change complete ranges for certain days of the week or time spans. ▪ To add ranges of check marks, use the buttons **All**, **Mo**, **Tu**, **We**, **Th**, **Fr**, **Sa**, and **Su**, as well as the time buttons on the left side.

Basic Settings	
	▪ To remove ranges of check marks, use the buttons **All Off**, **Mo Off**, **Tu Off** , **We Off**, **Th Off**, **Fr Off**, **Sa Off**, and **Su Off**, as well as the time **Off** buttons on the right side.

Inherit Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: • **Inherited**: Use the settings of the parent object. • **None**: Users in this group cannot see or edit the object. The object does not show up in lists. • **Read**: Users in this group can see the object and review its settings. • **Write**: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. • **Full**: Users in this group can see the object, as well as review and edit its settings and edit access rights settings. You can create new user groups in the System Administration—User Groups 887 settings.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

© 2011 Paessler AG

7.12.4 System Administration—System and Website

In the system and website settings you can define global values regarding the PRTG system, web site appearance, and web server settings and performance.

System & Website Settings

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Webserver and Website Settings	
Web Server IP Address	This is the IP address the PRTG web server is running on. This setting is shown for your information only and cannot be changed here. To change this setting, please use the PRTG Server Administrator 955.
Web Server Port	This is the port number the PRTG web server is running on. This setting is shown for your information only and cannot be changed here. To change this setting, please use the PRTG Server Administrator 955.
PRTG Site Name	When using the web interface, the site name is shown in the title bar of your browser window. It is also used by default in notification emails. Please enter a string.
DNS Name	If your PRTG web interface is (additionally) reachable via a DNS name, please enter it here. It is e.g. used by default in notification emails to generate links. Please enter a string.
Graph Type	Select how graphs are displayed throughout the web interface and in reports 827. ▪ **Use area charts (recommended)**: Display filled graphs. ▪ **Use line charts**: Display graphs using single lines only. We recommend using area charts, as they're better to read. *Note:* Graphs containing data from more than one cluster node will always be displayed with line charts automatically.
Background Color for Graphs	Select a background color for all graphs throughout the web interface and in reports 827. Either enter a hex color code or choose a color from the color selector. The hex color code field will always display the currently defined color.
Performance Strategy	Select if you want to enable performance improvements for the web interface. ▪ **All Features: Show all features and live data (recommended)**: Provide full functionality and show all menu items. ▪ **More Speed: Limit features and delay display (experimental)**: Improve reaction time and speed of the web interface by delaying display of monitoring data and hiding some features. For more information on how to speed up the web interface, please see **More** 876 section below.

Webserver and Website Settings	
Session Expiry	Select the idle time after which a user is automatically logged out of the web interface. Choose between: ▪ **15 Minutes** ▪ **1 Hour** ▪ **3 Hours** ▪ **6 Hours** ▪ **12 Hours** ▪ **1 Day** ▪ **Never** *Note:* PRTG's automatic page refresh function will avoid automatic logouts.
PDF Engine for Reports	Define how report PDFs will be generated. Choose between: ▪ **Use Webkit-based PDF engine (recommended)** ▪ **Use Internet Explorer installed on PRTG Core Server (deprecated)** We recommend using the webkit-based engine in order to generate reports independent of the Internet Explorer version installed on the computer running the PRTG core server. *Note:* If the deprecated option is selected, Internet Explorer version 8 has to be installed on the system running the PRTG core server, so PRTG's PDF report generation can work correctly. If PRTG detects an Internet Explorer 9 installed on the system, always the webkit engine will be used regardless of the selected option.
Feedback Links	In a PRTG installation running on a commercial license key, usually, a feedback link is displayed in the lower right corner, enabling you to send us comments about our software any time. You can switch this feature off an on. Choose between: ▪ **Show feedback links for all users (except read only users)**: Show feedback links for all users with write access. The links will never be shown for users set to read only. ▪ **Hide feedback links for all users**: Do not show feedback links. This setting is valid for all user accounts.

Geo Maps (Google Maps Integration)	
Map Type	Select if and how you want to integrate the Google Maps feature into the web interface. If enabled, PRTG uses the first line of the location setting of an object 111 to show it on a geographical map. ▪ **Do not show maps (disables Google Maps integration)**: Disable Google Maps integration and do not show geographical maps in the web interface. ▪ **Road Map**: Display graphical road maps. ▪ **Satellite**: Display photographic satellite maps. ▪ **Terrain**: Display geographical terrain maps. ▪ **Hybrid (Satellite and Road Map)**: Display maps mixed of satellite and road maps. For more information please see the **More** 876 section below.

© 2011 Paessler AG

Geo Maps (Google Maps Integration)	
Google Maps API Key (required)	In order to use Google Maps in PRTG you must agree to the Google Maps Terms of Service and apply for your personal *Maps API Key*. Please paste your key here. To apply for a free key, simply click on the link provided within the help text on the right side. For more information on how to get an API key, please see the **More** 876 section below.

Scanning Intervals	
Available Intervals	Define the intervals available in the drop down list of every object's settings 111. In the text field, enter one value in each line. Use **s**, **m**, **h**, and **d** for defining seconds, minutes, hours, and days. By default, there are following scanning intervals defined: **30s**: 30 seconds **1m**: 1 minute **5m**: 5 minutes **10m**: 10 minutes **15m**: 15 minutes **30m**: 30 minutes **1h**: 1 hour **4h**: 4 hours **6h**: 6 hours **12h**: 12 hours **1d**: 1 day *Note:* We recommend to not use intervals shorter than 10 seconds to prevent system overload. Intervals below 10 seconds are not officially supported!

Uptime Threshold	
Minimum Allowed Uptime Threshold	Define which uptime in percent will be regarded as 100 percent. This setting affects the colors shown next to the sensor icons in reports. Select one of the predefined values between **90 %** and **99.999 %**.

Email Options	
Email Templates	Choose which templates will be used for all emails sent. ▪ **Use New PRTG 8 Templates (Recommended)**: Use this option if you are not sure what to use. These templates offer the best compatibility with all email clients. ▪ **Use Old PRTG 7 Templates (for upgrade installations only)**: This option is provided for upgrade installations only. Use it if you have updated from PRTG version 7 and really want to continue using the old email templates. This can be useful when using custom HTML templates in PRTG 7 format. Depending on the option selected, the content of the other fields in this section changes.

Email Options	
Email Header (HTML)	Define the HTML text that will be used as the header for each HTML mail. To reset this field to its default value, enter a single star symbol * (and nothing else). Click on the **Reset to default** link underneath the text box to do so.
Email Footer (HTML)	Define the HTML text that will be used as a suffix to every HTML mail. To reset this field to its default value, enter a single star symbol * (and nothing else). Click on the **Reset to default** link underneath the text box to do so.
For Text Mails	Select if a footer will be added to plain text mails. Choose between: ▪ **Append text footer (default)**: Add a text footer to all text mails. Define the text below. ▪ **Do not append the footer Append text footer**: Do not add a footer to text mails.
Email Footer (Text)	Define a text that will be used as a suffix to every plain text mail (if enabled above). You can use several placeholders in email templates. See the More 876 section below for more information. To reset this field to its default value, enter a single star symbol * (and nothing else). Click on the **Reset to default** link underneath the text box to do so.
For New ToDos	Select what will be done when there are new ToDos 117. Choose between: ▪ **Do not send an email**: Do not send out any mail indicating that there is a new ToDo. ▪ **Send an email to admin account**: Send an email to the default administrator email address defined in the PRTG Server Administrator 955. ▪ **Send an email to specific address**: Define a custom email address ToDo notifications will be sent to.
ToDo Mail Address	This option is only visible if a specific address for ToDo mails is enabled above. Enter a valid email address ToDo notifications will be sent to.

Data Purging Limits: Select for how many days historic data remains accessible	
Data purging enables you to automatically delete unnecessary data to free up disk space and improve system performance. You can define different time spans for several kinds of data. For further information on storage locations, please see the More 876 section below.	
Logfile Records	Define how long records in the system logfile *Log Database.db* will be kept. Enter a value in days. All entries older than this value will be deleted from the log file automatically. Keep this value as low as possible to enhance system performance.
Web Server Log Records	PRTG creates one web server log file every day. Define how many web server log files will be kept. Enter a value in days. All web server log files files older than this value will be deleted automatically.

© 2011 Paessler AG

Data Purging Limits: Select for how many days historic data remains accessible	
Historic Sensor Data	Define for how many days historic sensor data will be kept for all sensors. It is used to create reports 827 of monitoring data. Enter a value in days. Depending on the used intervals and the number of sensors in your setup, the file containing this data can become large. For smaller installations (500 sensors or less) a value of 365 should be fine. Historic sensor data is the basis for reports on monitoring data. If you decrease this value, there will be less historic monitoring data available!
Toplist Records	Define how long toplist records will be kept. Enter a value in days.
ToDo Records	Define how long ToDo entries will be kept. Enter a value in days.
Reports	Reports generated in PDF format are stored on disk for later reference. Define the maximum age for these reports. Enter a value in days. All reports older than this value will be deleted automatically.
Configuration Auto-Backups	PRTG creaes one backup of your configuration every day. Define the maximum age for these backups. Enter a value in days. All configuration backup files older than this value will be deleted automatically.

Unusual Detection	
The unusual detection can set sensors to an **Unusual** status 102 when there are values that are untypical for the time span they're measured in, compared to historic monitoring results. When disabled (both settings to **Never**), sensors will never be shown as unusual.	
Show Unusual When	Define when a sensor will be shown as unusual, comparing the weekday. Choose between: ▪ **Never**: Disable unusual detection for weekday average. ▪ **24h average is <80% or >120% of weekday average** ▪ **24h average is <50% or >200% of weekday average** ▪ **24h average is <20% or >500% of weekday average (recommended)** ▪ **24h average is <10% or >1,000% of weekday average** ▪ **24h average is <1% or >10,000% of weekday average**
Show Unusual When	Define when a sensor will be shown as unusual, comparing the hour-of-day. Choose between: ▪ **Never**: Disable unusual detection for hour-of-day average. ▪ **24h average is <80% or >120% of hour-of-day average** ▪ **24h average is <50% or >200% of hour-of-day average** ▪ **24h average is <20% or >500% of hour-of-day average (recommended)** ▪ **24h average is <10% or >1,000% of hour-of-day average** ▪ **24h average is <1% or >10,000% of hour-of-day average**
Logging	Define if unusual events will be written to the log file. Choose between: ▪ **Do not log unusual events** ▪ **Write unusual events into the log**

Auto-Discovery Settings	
Specific Hour	Auto-discoveries can produce a certain load, so you can define at which hour of the day auto-discoveries 145 should be run when configured on a daily or weekly **Discovery Schedule**. Choose a full hour between **0:00** and **23:00**.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: What placeholders can I use with PRTG?
- http://www.paessler.com/knowledgebase/en/topic/373

Knowledge Base: How can I speed up PRTG—especially for large installations?
- http://www.paessler.com/knowledgebase/en/topic/2733

Knowledge Base: How do I get an API Key in order to use Google Maps with PRTG?
- http://www.paessler.com/knowledgebase/en/topic/17093

Knowledge Base: Can I avoid the "page contains insecure content" popups for PRTG 8 Geo Map feature?
- http://www.paessler.com/knowledgebase/en/topic/7333

Knowledge Base: Which limitations apply when using the Google Maps API in PRTG?
- http://www.paessler.com/knowledgebase/en/topic/7913

Knowledge Base: How and where does PRTG store its data?
- http://www.paessler.com/knowledgebase/en/topic/463

© 2011 Paessler AG

7.12.5 System Administration—Notification Delivery

In the notification delivery settings you can define global settings for notification delivery. If you do not want to use a specific notification method, just leave the respective fields empty.

Note

This section describes one of three steps to set up the notification system in PRTG. A complete notification setup involves:

1. Defining notification delivery settings
2. Setting up notifications
3. Adding notification triggers to sensors

For more information please see Notifications 826 section.

Notification Delivery Settings

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

SMTP Delivery	
SMTP Delivery Mechanism	Define how mails are sent using Simple Mail Transfer Protocol (SMTP). Choose between: ▪ **Direct delivery using built-in mail relay server (default)**: Use the SMTP relay server built into PRTG. ▪ **Use SMTP relay server (recommended inside LANs/NATs)**: Set up you own SMTP relay server to send emails. Enter data below. ▪ **Use two SMTP relay servers (primary and fallback server)**: Set up two own SMTP relay servers—one primary and one as fallback server. Enter data below. *Note:* When monitoring inside your NAT or LAN it is often a good idea to use your own LAN-based relay server to deliver notification emails quicker.
Sender Email	Enter an email address that will be used as sender of all emails. This setting is global and can only be changed centrally here.
Sender Name	Enter a name that will be used as sender of all emails. This setting is global and can only be changed centrally here.
HELO Ident	Enter the HELO Ident for SMTP. This must be a unique name, preferably the DNS name of the machine running PRTG. See SMTP RFC 2821: *The sender-SMTP must ensure that the domain parameter in a HELO command is a valid principal host domain name for the client host.*
SMTP Relay Server	This field is only visible if SMTP relay server is enabled above. Enter the IP address or DNS name of the SMTP relay server.

SMTP Delivery	
SMTP Relay SMTP Port	This field is only visible if SMTP relay server is enabled above. Enter the port number the SMTP relay server is running on. Standard value is **25**.
SMTP Relay Authentication	This field is only visible if SMTP relay server is enabled above. Select the kind of authentication required for the SMTP server. Choose between: ▪ **No authentication is required**: Use SMTP without authentication. ▪ **Use standard SMTP authentication**: Use standard authentication. ▪ **SASL authentication is required**: Use secure authentication via Simple Authentication and Security Layer (SASL).
SSL Method	This setting is only visible if SMTP relay server is enabled above. It is only relevant for secure connections. Select the SSL method to use. We recommend using the default value. If you do not get a connection, try with another setting.
SMTP Relay Username	This field is only visible if SMTP authentication is enabled above. Enter a valid user name.
SMTP Relay Password	This field is only visible if SMTP authentication is enabled above. Enter a valid password.
Security	This field is only visible if SMTP relay server is enabled above. Enter the security level for SMTP connections. Choose between: ▪ **No encryption (use plain text):** Use insecure connection with plain text transfer. ▪ **Encrypt data using Transport-Level Security (TLS):** Use a secure connection.
SMTP Relay Server (Fallback)	These fields are only visible if the option for two SMTP relay servers is enabled above. Please see respective settings for primary SMTP relay server above.
SMTP Relay SMTP Port (Fallback)	
SMTP Relay Authentication (Fallback)	
SSL Method (Fallback)	
SMTP Relay Username (Fallback)	
SSL Method (Fallback)	
SMTP Relay Username (Fallback)	
SMTP Relay Password (Fallback)	
Security (Fallback)	

© 2011 Paessler AG

SMS Delivery	
Configuration Mode	Define how you want to select an SMS provider. Choose between: ▪ **Select a SMS provider from a list of providers**: Select a provider from a list below. ▪ **Enter a custom URL for a provider not listed**: Use another provider and enter the service URL manually below.
Service Provider	This field is only visible if the provider list is enabled above. Choose a service provider from the list. PRTG offers a small incomplete list of providers. *Note:* Some providers might require a port configuration in your firewall. See More 880 section below for more information.
Username	This field is only visible if the provider list is enabled above. Enter a user name for the service provider account.
Password	This field is only visible if the provider list is enabled above. Enter a password for the service provider account.
API ID / Account	This field is only visible if the provider list is enabled above. Some providers need an additional API ID or account information. If provided, enter it here. Please enter a string or leave the field empty.
Custom URL	This field is only visible if the custom provider option is enabled above. From the documentation of your SMS provider, please enter the service URL that is used to send SMS messages. Use the following placeholders for the recipient phone number and the text message: **%SMSNUMBER**, **%SMSTEXT**.

Note: Although PRTG has built-in support for the Application Programming Interface (API) of some SMS providers, we cannot officially provide support regarding these SMS service providers. If you have technical questions about SMS delivery beyond PRTG, please contact your SMS provider directly.

You need an Internet connection to send text messages via the HTTP API. For information about sending SMS via separate hardware using third party software, please see the More 880 section below.

HTTP Proxy	
Name	If you want to use a proxy for notification delivery, please enter the IP address or DNS name of the proxy. To not use a proxy, leave the field empty.
Port	Enter the port the proxy is running on.
User	If required, enter a user name for proxy login. Please enter a string or leave the field empty.
Password	If required, enter a password for proxy login. Please enter a string or leave the field empty.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: How can I send SMS text message notifications via a modem or a mobile phone with PRTG?

- http://www.paessler.com/knowledgebase/en/topic/393

Knowledge Base: Why do I get a connection timeout message when sending SMS via bulksms?

- http://www.paessler.com/knowledgebase/en/topic/12253

Knowledge Base: Which URLs does PRTG use for its preconfigured SMS providers?

- http://www.paessler.com/knowledgebase/en/topic/13123

Knowledge Base: How can PRTG send instant messages to Jabber, ICQ, MSN, Yahoo, etc., using external software?

- http://www.paessler.com/knowledgebase/en/topic/14803

© 2011 Paessler AG

7.12.6 System Administration—Probes

In the probe management settings you can define the settings for probe connections.

Probes Settings

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Probe Connection Settings	
Access Keys	Enter a list of access keys, one in each line. Every (remote) probe that want to connect to this PRTG installation has to use one of these keys. For information how to set this key for a probe, please see PRTG Probe Administrator 969 (Probe Settings) section.
Allow IPs	Enter a list of remote probe IPs that will be accepted when connecting to this PRTG installation; each IP address in one line. The local probe (*127.0.0.1*) is always allowed automatically. Allowed IPs are checked first (before denied IPs). You can use PRTG's syntax for IP address ranges here (for information about the syntax please see Define IP Ranges 984 section). ▪ ***[Empty]***: An empty field does not allow any remote probes (but only the local probe). Please enter IP addresses to allow remote probe connections. ▪ **any**: Enter the word **any** to automatically allow all remote probe connections. *Note:* This is recommended for use in Intranets only! *Note:* If the IP address of your remote probe changes regularly (e.g. due to an Internet provider assigning IP addresses dynamically), please enter the potential IP range for this remote probe or use the **any** option.
Deny IPs	Enter a list of remote probe IPs that will *not* be accepted when connecting to this PRTG installation; each IP address in one line. This is useful to explicitly deny connections from certain remote probes you do not want to include in your setup any more (e.g. for a certain time). Access to IP addresses allowed above will be denied if you enter them here. This is useful to allow access to an IP range in the field above, but deny access to a single IP address. You can use PRTG's syntax for IP address ranges here (see More 882 section below).

Settings from the PRTG Server Administrator program	
IPs for Probe Connections	This is a list of the IP addresses on which the PRTG listens to incoming probe communication. **0.0.0.0** means that the server listens on all local network adapter IPs. This setting is shown for your information only and cannot be changed here. To change this setting, please use the PRTG Server Administrator 955.

Settings from the PRTG Server Administrator program	
Probe Connections Port	This is the port on which PRTG listens to incoming probe communication. This setting is shown for your information only and cannot be changed here. To change this setting, please use the PRTG Server Administrator 955.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Remote Probe Setup

Find more information about setting up remote probes in the **Multiple Probes and Remote Probes** 986 section.

More

- **Define IP Ranges** 984

© 2011 Paessler AG

7.12.7 System Administration—Cluster

In the cluster settings you can define the cluster settings. During installation of a cluster 53, the cluster settings were already pre-defined. See the cluster status 888 to see if all nodes in your cluster are properly connected.

Cluster Settings

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

You can set up two, three, four, or five nodes in one cluster. In the table of the cluster settings, the information of each node is written in one line.

Node Settings	
Node Name	Enter the name of the node (for display purposes).
Node ID	The ID is unique for every node. We recommend using the default value.
Node State	You can set the state for every failover node. Choose between: ▪ **Active**: Set the node to be active. ▪ **Inactive**: Set the node to be not active. It will be disabled in the cluster configuration. It will then be not an active part of the cluster and will not appear in the cluster status 888 any more. This setting is not available for the master node of a cluster. The master is always set to **Active**.
IPs/DNS Names used for Connections Between Nodes	Define the IP addresses or DNS names that will be used for the connections between the nodes. You can enter different values for every node–node connection. For example, in the field **#2 => #1**, enter the IP address that the second cluster member (this is a failover node) will use to connect to the master node server.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

In order to put a cluster node to **Maintenance Mode**, please see **PRTG Status—System Status** 888.

The entire setup process for a cluster requires several different steps. For more information and step-by-step guidance, please see **Install a PRTG Cluster** 53 section.

7.12.8 System Administration—User Accounts

PRTG administrator users can change all users' account settings and add new users.

- To change a user's settings, select it from the list by clicking on the user name. The available setting options are the same as shown in the **My Account** settings of the currently logged in user (plus some account control options).
- To add a new user, click on the **Add User** button. The options are the same as for existing users (with slight differences).

User Accounts Settings

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

User Account	
Login Name	Enter the login name for the user.
Username	Enter a name for the user for display purposes. This will not be used for login.
Email Address	Enter the user's email address.
Timezone	Enter the time zone for the current user.
Date Format	Enter in what format dates will be displayed for the current user.
Password	Define the user's password. For security reasons, the account settings page does not contain the password. Choose between: ▪ **Don't change** ▪ **Specify new password** If you choose to specify a new password, enter the old password, and the new password twice.
Hash	The hash (passhash) value can the used as password substitute when calling functions from PRTG's Application Programming Interface (API) that require an authentication. For more information please see Using the PRTG API (Application Programming Interface) 979 section.

Auto Refresh and Alerting	
Auto Refresh Type	Specify how PRTG's web pages will be refreshed for the current user. Choose between: ▪ **Refresh page elements using AJAX (recommended)**: Automatically refresh the single page elements on the web pages. ▪ **Refresh whole page**: Automatically reload the whole page with every refresh interval. ▪ **No auto refresh**: Do not automatically refresh web pages.

© 2011 Paessler AG

Auto Refresh and Alerting	
Auto Refresh Interval (sec)	This setting is only relevant when auto refresh is enabled above. Enter the number of seconds that will be waited between two refreshes. We recommend using **30** seconds or more. Minimum value is 20 seconds. *Note:* Shorter intervals create more CPU load on the server running the PRTG core server. If you experience load problems while using the web interface (or PRTG maps 842), please set a higher interval.
Play Audible Alarms	Define when an audible alarm will be played for the current user on web pages whenever there are alarms 113 in PRTG. Choose between: ▪ **Never**: Do not play sound files on any web pages. ▪ **On dashboard pages only**: When there are alarms, play a predefined sound on dashboard 133 pages only. The sound will be replayed with every refresh of a dashboard page. ▪ **On all pages**: When there are alarms, play a predefined sound on all web pages. The sound will be replayed with every page refresh. For more information about audible notifications and supported browsers, please see **More** 861 section below.

Web Interface	
Homepage URL	Define the user's default page loaded after login and when clicking on the Home 133 button in main menu.
Max. Groups/Devices per Group	In order to provide you with a speedy user experience PRTG tries to keep the page size for the page showing sensor trees small by automatically folding groups and devices with many items. Define how many groups and devices are shown at maximum before the automatic reduction is performed. We recommend using a value between **10** and **30**.
Max. Sensors per Device	In order to provide you with a speedy user experience PRTG tries to keep the page size for the page showing sensor trees small by automatically folding groups and devices with many items. Define how many sensors are shown at maximum before the automatic reduction is performed. We recommend using a value between **10** and **30**.

Account Control	
Account Type	This setting is only shown for administrator users. Define the account type for the current user. Choose between: ▪ **Read/Write User**: The user may change settings. ▪ **Read Only User**: The user may not edit any settings. This is a good choice for public or semi-public logins. *Note:* This setting cannot be changed for the default administrator user.
Primary Group	This setting is only shown for administrator users. Select the primary group for the current user. Every user has to be member of a primary group to make sure there is no user without group membership. Membership in other user groups is optional. For user experience, there is no difference between the primary and other user groups.

Account Control	
Status	This setting is only shown for administrator users. Define the status of the current user. Choose between: ▪ **Active**: The current user can login to the account. ▪ **Inactive**: The current user's login is disabled. Use this option to temporarily deny access for this user. *Note:* This setting cannot be changed for the default administrator user.
Last Login	Shows the time stamp of the user's last login. This setting is shown for your information only and cannot be changed here.

User Groups	
Member of	Shows the groups the current user is member of. Access rights to the device tree are defined on group level. This setting is shown for your information only and cannot be changed here.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: How can I setup audible notifications (sound files) in PRTG?
▪ http://www.paessler.com/knowledgebase/en/topic/5473

© 2011 Paessler AG

7.12.9 System Administration—User Groups

PRTG administrator users can change existing user groups or add new ones, and define the users that are member of a certain group.

All the security settings as well as further rights management are conducted via the user groups. This means that group membership controls what a user may do and which objects he/she sees when logged in. The actual rights for each object can be defined in an object's settings. There, you can define different rights for each user group.

- To change a user group's settings, select it from the list by clicking on the group name.
- To add a new user group, click on the **Add User Group** button. The options are the same as for existing users (with slight differences).

User Groups Settings

Note: This documentation refers to the **PRTG System Administrator** user using the Ajax interface on a master node. For other users, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

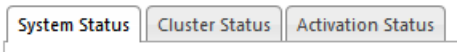
User Group Settings	
User Group Name	Enter a name for the user group.

User List	
Members	Define which users that will be a member of this group. To add a user from the list, add a check mark in front of the user name. The available users depend on your setup.

Primary Users	
User List	Shows a list of all users with this group set as primary group. This is shown for information purposes only. You can change it in a user's settings 884.

7.12.10 PRTG Status—System Status

To view the status of your PRTG installation, select **Setup | PRTG Status** from main menu. Click on the tabs to change the different settings.



PRTG Status Tabs

You can view the following aspects of the PRTG status:

- PRTG Status—System Status 888
- PRTG Status—Cluster Status 888
- PRTG Status—Activation Status 889

System Status

Click on the **System Status** tab to view relevant system information you may need for debugging or when the support team asks you to provide system information in order to support you with PRTG. Following information is shown:

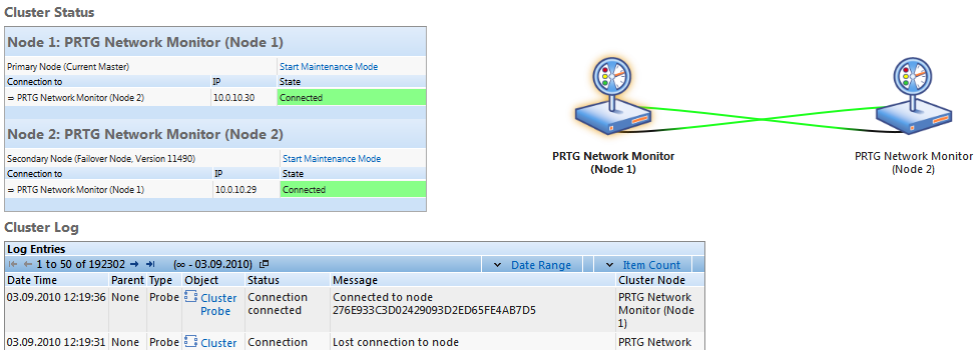
- Software Version and Server Information
- Licensing Information
- System Startup Log
- Cluster Status
- Local Status
- Cluster Connections
- Database Objects
- Probes
- System Settings
- Synchronization
- Background Tasks
- System Warnings
- Core System Memory
- Thread Information

Cluster Status

Click on the **Cluster Status** tab to view all nodes connected to the cluster. Following information is shown:

- Cluster Status with all connected nodes as table and graphic
- Cluster Log with all log entries concerning cluster connections

© 2011 Paessler AG



PRTG Cluster Status

Click on the **Start Maintenance Mode** link to put a cluster node in maintenance mode. A node in this mode is still connected to the cluster, but its monitoring results are discarded until you click on the **Stop Maintenance Mode** link. You can use this functionality to explicitly exclude a node from monitoring if you know that the monitoring values will not be accurate, for example, because you're reconfiguring things, etc. During maintenance, a cluster node is displayed with a transparent color in the overview graphic.

For more information about cluster settings, please see System Administration—Cluster 883 section.

Activation Status

Click on the **Activation Status** tab to view your license's activation status. For more information about activation, please see Activate the Product 57 section.

7.12.11 Downloads

To see optional downloads, select **Setup | Downloads** from main menu. Click on the tabs to switch between different options.

Downloads Tabs

There are the following downloads available:

- PRTG Windows GUI 890
- iPRTG iPhone App 890
- Remote Probe Installer 890
- PRTG Add-Ons 890
- PRTG Billing Tool 890

PRTG Windows GUI

Download the Windows Graphical User Interface (GUI) to the current system. Using it, you can access the PRTG interface with a native Windows application. The version of the Windows GUI must match your version of PRTG. For more information, please see **Install the Windows GUI** 64 section.

iPRTG iPhone App

iPRTG is a native iPhone application that enables you to use the PRTG web interface with the original iFeeling. You can buy iPRTG in the AppStore. For more information, please see **More** 891 section below.

Remote Probe Installer

With remote probes you can extend your monitoring to distributed networks that are not directly reachable from your PRTG core installation. The version of the remote probe installer must match your version of PRTG. For more information, please see **Install a PRTG Remote Probe** 59 section.

PRTG Add-Ons

There are many add-ons available from the PRTG community at a project hosting site. You can find special sensors and other software pieces there. Please follow the link to Google Code and have a look. *Note:* The provided add-ons come from third parties and are not officially supported as part of the PRTG software.

PRTG Billing Tool

The PRTG Billing Tool is an application that can read PRTG sensor data and generate bills in PDF format. It is an Open Source project which uses .NET and Lua scripting; monitoring data is queried via PRTG's built-in application programming interface (API). For more information, please see **More** 891 section below.

© 2011 Paessler AG

More

Paessler Website: Mobile Network Monitoring with the iPhone
- http://www.paessler.com/iprtg

Project Hosting on Google Code: PRTG AddOns
- http://code.google.com/p/prtg7addons/

Paessler Website: Billing Tool for PRTG
- http://www.paessler.com/tools/billingtool

Part VIII

Windows GUI

8 Windows GUI

The Windows GUI is one alternative interface you can use to connect to the PRTG core server to view monitoring results and keep an eye on your network. It is a native Windows application for fast access to data and provides extended popup window functionalities as well as a seamless link to the Ajax web interface 92 where you can change your monitoring configuration and access further functionalities such as reporting, system setup, etc.

With an installation of PRTG Network Monitor, the Windows GUI is included and installed automatically on the computer running the PRTG core server. If you want to use the Windows GUI on another computer, please download and install it there, as described in the **Install the Windows GUI** 64 section.

Note: The Windows GUI is mainly designed to review and manage an existing installation of PRTG which has already been set up. If you just started monitoring, we recommend you use the web interface's auto-discovery 145 function and add your network's devices there. For detailed instructions, please see **Quick Start Guide** 26 section. Once finished, you can seamlessly switch to the Windows GUI.

The following sections introduce the features and concepts of the Windows Graphical User Interface (GUI).

Windows GUI—Topics

- First Start 895
- General Layout 897
- Menu Tabs and Page Content 899
- Options and Server Settings 913
- Windows Menu Structure 919
- Context Menus 922
- Shortcuts Overview 923

Related Topics

- Ajax Web Interface—Basic Procedures 92
- Ajax Web Interface—Device and Sensor Setup 144
- Ajax Web Interface—Advanced Procedures 806
- Other User Interfaces 926

© 2011 Paessler AG

8.1 First Start

This section will help you starting the Windows GUI for the first time.

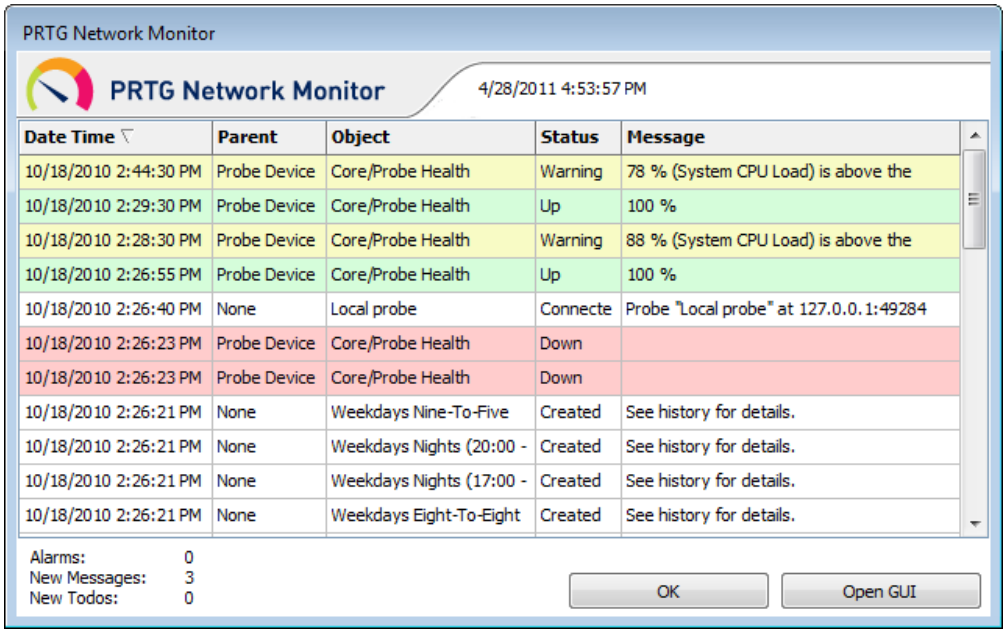
Opening the Windows GUI

Double click the **PRTG Windows GUI** icon in the Windows start menu to open it. As soon as it opens, the Windows GUI will try to connect to your PRTG installation, according to the given PRTG server connection settings. In a fresh install of PRTG, the settings are already predefined, so you can use the Windows GUI right away. If you get an error message when opening the Windows GUI, please check the connection settings. For example, editing the settings is necessary in case the IP address of the server has changed.

If you get an error message, please check your connection settings. For detailed information, please see Options and Server Settings 915 (**PRTG Server Connection**) section.

Popup Window

By default, the Windows GUI runs in the background and shows a popup message whenever there are new alerts, new messages, or new ToDos for your monitoring. It will be one of the first things you see after opening the GUI.


PRTG Network Monitor
PRTG Network Monitor
4/28/2011 4:53:57 PM
Date Time
Parent
Object
Status
Message
10/18/2010 2:44:30 PM Probe Device Core/Probe Health Warning 78 % (System CPU Load) is above the
10/18/2010 2:29:30 PM Probe Device Core/Probe Health Up 100 %
10/18/2010 2:28:30 PM Probe Device Core/Probe Health Warning 88 % (System CPU Load) is above the
10/18/2010 2:26:55 PM Probe Device Core/Probe Health Up 100 %
10/18/2010 2:26:40 PM None Local probe Connecte Probe "Local probe" at 127.0.0.1:49284
10/18/2010 2:26:23 PM Probe Device Core/Probe Health Down
10/18/2010 2:26:23 PM Probe Device Core/Probe Health Down
10/18/2010 2:26:21 PM None Weekdays Nine-To-Five Created See history for details.
10/18/2010 2:26:21 PM None Weekdays Nights (20:00 - Created See history for details.
10/18/2010 2:26:21 PM None Weekdays Nights (17:00 - Created See history for details.
10/18/2010 2:26:21 PM None Weekdays Eight-To-Eight Created See history for details.
Alarms: 0
New Messages: 3
New Todos: 0
OK
Open GUI

Example of a Popup Window

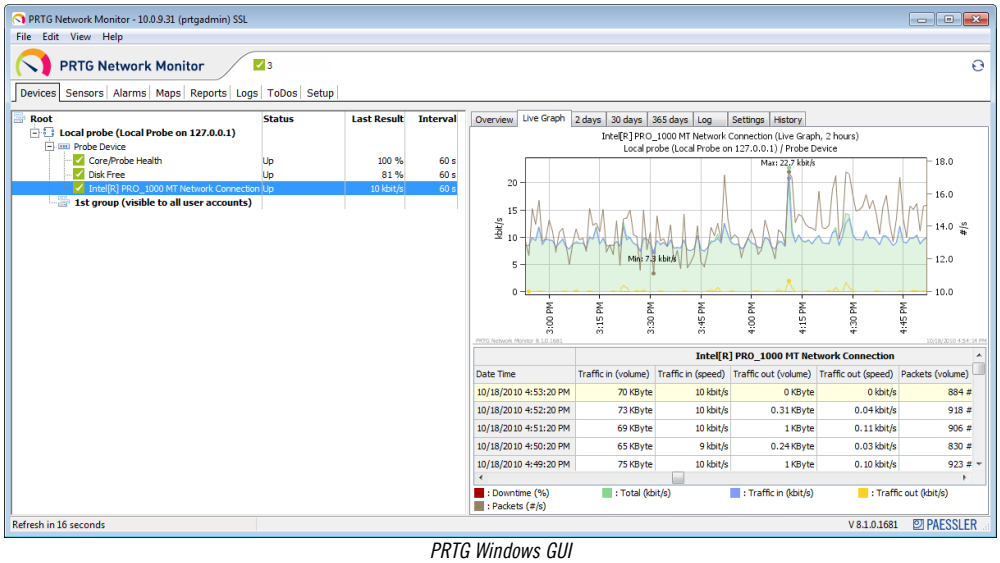
This window is shown as always on top. Click on the **OK** button to close it. You can change the popup behavior in the Windows GUI settings.

For detailed information, please see Options and Server Settings 914 (**System—Alerting**).

© 2011 Paessler AG

8.2 General Layout

The main layout of the Windows GUI program consists of different elements which will be shortly described here.



PRTG Windows GUI

From top to bottom, the main layout consists of:

- The Windows menu 897.
- The page header bar 897 with the PRTG logo, the sensors overview, and the refresh icon.
- The menu tabs bar and page content 898 underneath.
- The status bar 898 at the bottom of the window.

Often, data and settings are displayed directly in the Windows GUI. For some functionalities and extended setup, a new window of the system's default browser is opened and the web interface 92 will show up. In this case, you'll be logged in to the web interface automatically via username and hash value 859. In your browser, it might be necessary to confirm the certificate used by PRTG's web server. For more information, please see **Login** 93 (section **Confirm Certificate for Https Connection**).

Windows Menu

The Windows menu gives access to general configuration and settings. Find a detailed description in the **Windows Menu Structure** 919 section.

Page Header Bar

Windows GUI's Page Header Bar

The page header consists of the following parts:

- **PRTG Logo**
  Click on the PRTG Network Monitor logo to open the Ajax web interface 92 in your system's default browser.

- **Global Sensor State Symbols**
  It shows the aggregated status of all sensors you have configured for monitoring, divided into different sensor states. Depending on the sensors' status you will see colored boxes with numbers which symbolize the sensors. For example, you can see how many sensors are in **Up**, **Down**, or **Warning** state. Click on a box to view a list of all sensors in the respective status. For a detailed description, please see **Sensor States** 102 section.

- **Refresh (Arrows Symbol)**
  Click on the refresh symbol (*F5*) any time to refresh the current screen. This will immediately query data for the current screen from the PRTG core server, just as the automatic refresh does, which can be configured in the **Options and Server Settings** 913.

Menu Tabs Bar and Page Content

You can navigate through your setup using the menu tabs bar. Please take a few minutes to familiarize yourself with all menu items. The page content underneath varies dependent on the selected menu tab. It shows various information about your monitored objects. For a detailed description of all tabs, please see the **Menu Tabs and Page Content** 899 section.

Status Bar

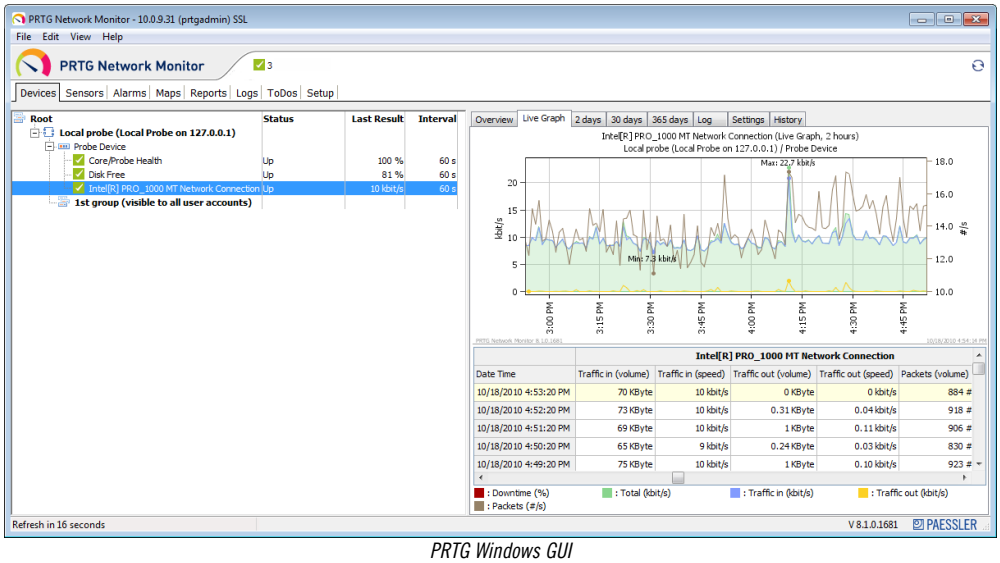
Windows GUI Status Bar

The status bar shows a countdown with the time to the next refresh, the version number of your PRTG installation and the Paessler logo which leeds you to the Paessler website when you click on it.

© 2011 Paessler AG

8.3 Menu Tabs and Page Content

Under the different menu tabs of the Windows GUI you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc.



PRTG Windows GUI

The following sections introduce the available options within the different tabs:

- Devices 900
- Sensors 904
- Alarms 906
- Maps 907
- Reports 908
- Logs 909
- ToDos 911
- Setup 912

8.3.1 Devices

The Windows GUI has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.

Windows GUI Menu Tabs Bar

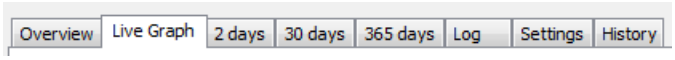
There is documentation for the following tabs:

- Devices 900
- Sensors 904
- Alarms 906
- Maps 907
- Reports 908
- Logs 909
- ToDos 911
- Setup 912

Devices Menu Tab

The **Devices** tab will be your starting point for everyday use. The page is split into two parts. On the left hand side, it shows the tree-like device view which lists all probes, groups, devices, and the sensors on the devices in a hierarchical order. For more information see Object Hierarchy 79 section. Next to each object you see an overview of the number of sensors, grouped by their current status.

On the right side you see details about the object selected on the left. The information is spread over several tabs.



Windows GUI Sub-Tabs on Devices Pages

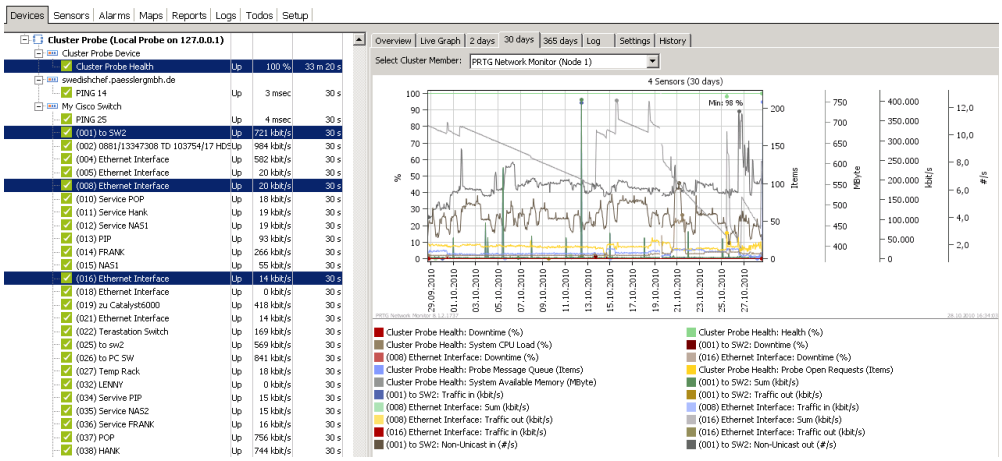
Select Multiple Items in Device Tree

In the device tree shown on the left, you can select one or more objects. Hold down the *Ctrl* key to select more objects simultaneously. Usually, you will select more than one item in order to apply a command from the Windows Menu 919 to several objects, or to view combined graphs.

When selecting multiple items, the sub-tabs on the right side will only show data for *all* selected items at a glace. For example, when selecting two sensors, you will see their tables next to each other. Graphs will actually be shown combined! This is a great way to instantly show one chart that contains all graphs of all selected objects. Each sensor channel will then be shown as one line. This aggregated view works for all kind of objects.

Underneath each graph a legend is shown. Hover an entry in the legend to display the according line in the graph above in **bold**.

© 2011 Paessler AG



Aggregated Graph View in Windows GUI

Note: You may need to enlarge the Windows GUI's window in order to see all tables and graphs.

Devices—Overview

The **Overview** tab shows general information about the selected object. Depending on the selected object, different information is displayed.

- For probes, groups, and devices, the table shows information in the **Name** section only, such as type and interval set, priority, and parent objects. On the right side, a geographical Map is shown, if enabled in your PRTG configuration as well as in the Windows GUI's View menu 921. For detailed information about geographical maps, please see Geo Maps 823 section.
- For sensors, additional information is displayed in the **Status** and **Channels** sections, such as the results of the last sensor scan.

Devices—Live Graph, 2 days, 30 days, 365 days

These tabs are only available if the **Large Single Graph** (*Ctrl+L*) view is enabled in the Windows Menu 921 (**View**). For **Small Multiple Graphs** view please see below 902.

Select one of the tabs **Live Graph**, **2 days**, **30 days**, or **365 days** to display an object's monitoring data live (content available for sensors only), or for different time spans and in more or less detail.

Select one of the tabs to display an object's monitoring results as **Live Graph** (content available for sensors only), or for different time spans in more or less detail (**2 days**, **30 days**, **365 days**). In every tab, you will see graphs as well as data tables. *Note:* The days mentioned here are the default setting. You can change the detail of the different graphs any time in the PRTG System Administrator program. See section PRTG Server Administrator 960 (Memory Usage) for more details.

Devices—Graph

This tab is only available if the **Small Multiple Graphs** (*Ctrl+S*) view is enabled in the Windows Menu 919 (**View**). For **Large Single Graphs** view please see above. This will show an overview with single graphs and data tables for live data, 2 days, 30 days, and 365 days. It might be necessary to enlarge the window in order to display all graphs. *Note:* The days mentioned here are the default setting. You can change the detail of the different graphs any time in the PRTG System Administrator program. See section PRTG Server Administrator 960 (Memory Usage) for more details.

Devices—Log

Click on the **Log** tab to show a table list with all log information *on this object*. This is a subset of the entries available via the Logs 909 menu tab.

In the list, one hundred entries are shown at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

Devices—Settings

In the **Settings** tab the currently selected object's settings are loaded from the web interface and displayed. View and functionality are the same as in the web interface. For every type of object and for every sensor, different options are available. For detailed information, please see the following sections (depending on the selected object):

- Probe Settings 173
- Group Settings 181
- Device Settings 193
- Sensor Settings 202

Note: When accessing this page, PRTG opens an embedded Internet Explorer window, showing a part of the Ajax web interface 92. You might see an Internet Explorer security warning stating that the used certificate is invalid. In a standard setup, the connection to the web interface is SSL-encrypted, using a certificate that is automatically installed with PRTG. Although the connection is securely encrypted, it is not a "trusted" certificate issued by a known entity. That is why this message is displayed. Please confirm the warning in order to proceed. For more information on secure browser connections, please see the More 96 section of the web interface documentation describing the login.

Settings for sensor channels and notification triggers can only be changed in the web interface. For detailed information, please see Object Settings 111 section.

Devices—History

In the **History** tab all changes in the settings of an object are shown with a timestamp, the PRTG user which conducted the change, and a message.

© 2011 Paessler AG

Drag & Drop Sorting

In the device tree, you can also move probes, groups, and devices simply via drag and drop. Activate it in the Windows menu 919 **Edit | Drag & Drop Sorting** and then drag your objects as you like.

8.3.2 Sensors

The Windows GUI has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.

Windows GUI Menu Tabs Bar

There is documentation for the following tabs:

- Devices 900
- Sensors 904
- Alarms 906
- Maps 907
- Reports 908
- Logs 909
- ToDos 911
- Setup 912

Viewing lists of sensors is a great way to keep an eye on your network's status, as you can select which kind of sensors you would like to see. You can filter by object, sensor type, and current sensor state.

Sensors Menu Tab

Click on the **Sensors** entry in the menu tabs bar to show a table list of all sensors. You can enable a filter to only show certain sensors. To do so, choose from three different drop down menus to build a filter. With each filter you can further decrease the number of sensors shown.

- **By Object**
  The first drop down menu shows the device tree of your monitoring setup. Select a probe, group, or device, in order to only show sensors on this object. The default value is **All Sensors**.

- **By Type**
  The second drop down menu shows all sensor types available in your monitoring setup. Select an entry to only show sensors of this type. The default value is **All Types**.

- **By State**
  The third drop down menu shows all possible sensor states. Select an entry to only show sensors that currently show this status. Choose between **All States**, **Down**, **Warning**, **Up**, **Paused**, **Unusual**, and **Unknown**. The default value is **All States**. *Note:* If you click on a sensor symbol in the page header bar 897, you can directly view a sensor list filtered by the selected sensor state.

If you have filtered out all sensors and the list below shows no entries, try removing some filters by reverting them to the default values. To disable all filters, remove the check mark in front of the **Filter by** option at the beginning of the line.

© 2011 Paessler AG

In the list, one hundred entries are shown at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

© 2011 Paessler AG

8.3.3 Alarms

The Windows GUI has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.

Windows GUI Menu Tabs Bar

There is documentation for the following tabs:

- Devices 900
- Sensors 904
- Alarms 906
- Maps 907
- Reports 908
- Logs 909
- ToDos 911
- Setup 912

Alarms Menu Tab

The Alarm list shows all sensors that are currently in a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. Sensors in other states (e.g. **Up**, **Paused**, or **Unknown**) do not appear here. This is useful to keep track of all irregularities in your network.

Using the options **Error**, **Warning**, and **Unusual**, you can hide and show sensors in the respective status by removing and adding a check mark. When choosing **Error**, this includes sensors in the states **Down**, **Down (Partial)**, and **Down (Acknowledged)**.

If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

Acknowledge Alarm

In order to acknowledge an alarm, right-click on a sensor and choose **Acknowledge Alarm...** from the context menu 922, enter a message and click the **OK** button. The message will appear in the sensor's last message value. An acknowledged alarm will not show up in the alarms list any more and will not trigger 797 any more notifications 825.

© 2011 Paessler AG

8.3.4 Maps

The Windows GUI has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.

Windows GUI Menu Tabs Bar

There is documentation for the following tabs:

- Devices 900
- Sensors 904
- Alarms 906
- Maps 907
- Reports 908
- Logs 909
- ToDos 911
- Setup 912

Maps Menu Tab

The page is split into two parts. On the left hand side, you see all available maps, on the right hand side the actual maps are displayed. Click on a map's name to display it. This is a view-only mode. You cannot edit maps here. In order to add new maps or edit existing ones, please use the web interface. For more information see Maps 842 section.

Note: When accessing this page, PRTG opens an embedded Internet Explorer window, showing a part of the Ajax web interface 92. You might see an Internet Explorer security warning stating that the used certificate is invalid. In a standard setup, the connection to the web interface is SSL-encrypted, using a certificate that is automatically installed with PRTG. Although the connection is securely encrypted, it is not a "trusted" certificate issued by a known entity. That is why this message is displayed. Please confirm the warning in order to proceed. For more information on secure browser connections, please see the More 96 section of the web interface documentation describing the login.

8.3.5 Reports

The Windows GUI has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.

Windows GUI Menu Tabs Bar

There is documentation for the following tabs:

- Devices 900
- Sensors 904
- Alarms 906
- Maps 907
- Reports 908
- Logs 909
- ToDos 911
- Setup 912

Reports Menu Tab

In the **Reports** tab you see all existing reports configured in your setup.

If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

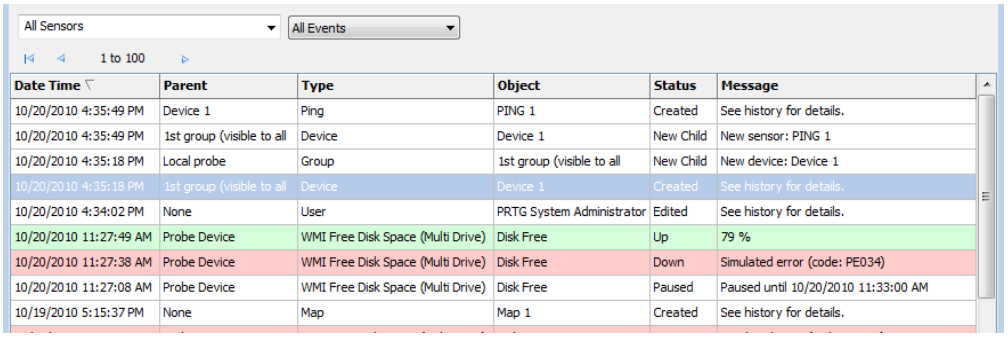
Double click on any report object in the table to run, open, or edit it. All report functionality is embedded in the web interface. For detailed information, please see Reports 827 section.

When you click on one of these items, a new window or tab of your system's default browser will open and PRTG will automatically login and redirect you to the respective web page. If your browser displays a certificate warning, please find more information in the Login 93 section (**Confirm Certificate for Https Connection**).

© 2011 Paessler AG

8.3.6 Logs

The Logs list shows all past activities and events of your PRTG monitoring setup. This is useful to keep track of all important activities and, for example, to check whether messages were sent, etc. In a typical setup, a huge amount of data is produced here. As the activity of every single object is minuted, you can use this data to check exactly if your setup works as expected.



Date Time	Parent	Type	Object	Status	Message
10/20/2010 4:35:49 PM	Device 1	Ping	PING 1	Created	See history for details.
10/20/2010 4:35:49 PM	1st group (visible to all	Device	Device 1	New Child	New sensor: PING 1
10/20/2010 4:35:18 PM	Local probe	Group	1st group (visible to all	New Child	New device: Device 1
10/20/2010 4:35:18 PM	1st group (visible to all	Device	Device 1	Created	See history for details.
10/20/2010 4:34:02 PM	None	User	PRTG System Administrator	Edited	See history for details.
10/20/2010 11:27:49 AM	Probe Device	WMI Free Disk Space (Multi Drive)	Disk Free	Up	79 %
10/20/2010 11:27:38 AM	Probe Device	WMI Free Disk Space (Multi Drive)	Disk Free	Down	Simulated error (code: PE034)
10/20/2010 11:27:08 AM	Probe Device	WMI Free Disk Space (Multi Drive)	Disk Free	Paused	Paused until 10/20/2010 11:33:00 AM
10/19/2010 5:15:37 PM	None	Map	Map 1	Created	See history for details.

Windows GUI Logs (Menu Tabs Bar)

There are two possibilities to call the logs list: Either you click on the **Log** tab while viewing an object's details in the Devices 902 menu tab, or you choose the **Logs** entry from the menu tabs bar.

Logs Menu Tab

The Windows GUI has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.

Windows GUI Menu Tabs Bar

There is documentation for the following tabs:

- Devices 900
- Sensors 904
- Alarms 906
- Maps 907
- Reports 908
- Logs 909
- ToDos 911
- Setup 912

Click the **Logs** entry in the menu tabs bar to show a list of *all* log entries in your configuration. The background color of a row indicates the value listed in the **Status** column. It is shown green for **Up**, yellow for **Warning**, red for **Down**, and white for all other values.

You can enable a filter to only show certain sensors. To do so, choose from two different drop down menus to build a filter. With each filter you can further decrease the number of sensors shown.

- **By Object**
  The first drop down menu shows the device tree of your monitoring setup. Select a probe, group, or device, in order to only show sensors on this object. The default value is **All Sensors**.

- **By Event**
  The second drop down menu shows all possible event types. Select an entry to only show events of the respective event type. Choose between **All Events**, **Up & Down**, **Warning**, **Unusual**, **Up**, **Paused & Resumed**, **Probe Related**, **Auto Discovery**, **Notifications**, and **Status Messages**. The default value is **All Events**.

If you have filtered out all sensors and the list below shows no entries, try removing one or both filters by reverting them to the default values.

In the list, one hundred entries are shown at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

© 2011 Paessler AG

8.3.7 ToDos

The Windows GUI has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.

Windows GUI Menu Tabs Bar

There is documentation for the following tabs:

- Devices 900
- Sensors 904
- Alarms 906
- Maps 907
- Reports 908
- Logs 909
- ToDos 911
- Setup 912

ToDos Menu Tab

The ToDos list shows items with important system information or action steps to take for the administrator.

New ToDos are created when:

- A new device or sensor has been created by the auto-discovery process and should be acknowledged by the user
- A new probe connects to the core and must be acknowledged
- A new cluster node connects to the cluster and must be acknowledged
- A new version of the software is available
- A new report is ready for review
- In a few other situations, such as when the system runs out of disk space, for licensing issues, etc.

The list shows all available ToDos. In order to acknowledge ToDos or change the email settings for them, log in to the web interface.

When you click on one of these items, a new window or tab of your system's default browser will open and PRTG will automatically login and redirect you to the respective web page. If your browser displays a certificate warning, please find more information in the Login 93 section (**Confirm Certificate for Https Connection**).

8.3.8 Setup

The Windows GUI has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.

Windows GUI Menu Tabs Bar

There is documentation for the following tabs:

- Devices 900
- Sensors 904
- Alarms 906
- Maps 907
- Reports 908
- Logs 909
- ToDos 911
- Setup 912

Setup Menu Tab

In the **Setup** tab you can access the **Account Settings** and **System Administration** of your PRTG setup. Every button on this page leads you to the web interface where you can edit the respective settings.

When you click on one of these items, a new window or tab of your system's default browser will open and PRTG will automatically login and redirect you to the respective web page. If your browser displays a certificate warning, please find more information in the Login 93 section (**Confirm Certificate for Https Connection**).

For more information please refer to the respective section in the web interface's documentation.

Account Settings:

- My Account 859
- Notifications 862
- Schedules 868

System Administration:

- System & Website 871
- Notification Delivery 877
- Probes 881
- Cluster 883 (only available in a cluster 78 setup)
- User Accounts 884
- User Groups 887

© 2011 Paessler AG

8.4 Options and Server Settings

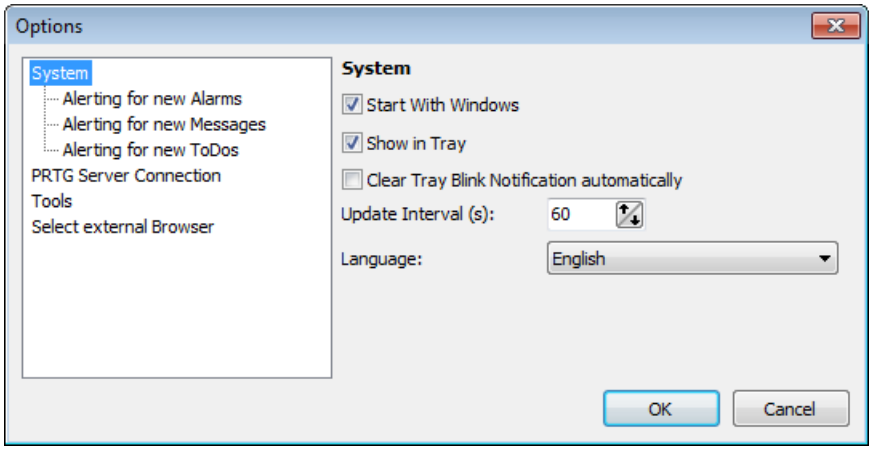
From the Windows menu 919, select **File | Options & Server Settings...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

You can choose from these options on the left hand side:

- System 913
- System—Alerting 914
- PRTG Server Connection 915
- Tools 916
- Select External Browser 918

System

Change general system settings for the Windows GUI.



Windows GUI Options and Server Settings

Start With Windows

- By default this setting is enabled.
- With this setting enabled, the Windows GUI will start up automatically when this computer is started.

Show in Tray

- By default this setting is enabled.
- With this setting enabled, a PRTG icon will be shown in the Windows tray.
- On mouse over, it will show a balloon info with the most important status information about your monitoring; with a right-click you can access a menu with access to the most important functions.
- In order to use any alerting functionalities (see System—Alerting 914 section), you must enable this option. If the tray icon is not shown, no alerting from the Windows GUI will be available.

Clear Tray Blink Notification automatically

- Whenever there are new alarms (sensors is **Down** status), the tray icon will start blinking. If you enable this option, the tray icon will stop blinking automatically as soon as there are no more alarms.
- With this option disabled, it will keep blinking, even if all alarms should be cleared meanwhile.

Update Interval (s)

- Define the number of seconds that will be waited before the screen is refreshed.
- Default value is **60**.

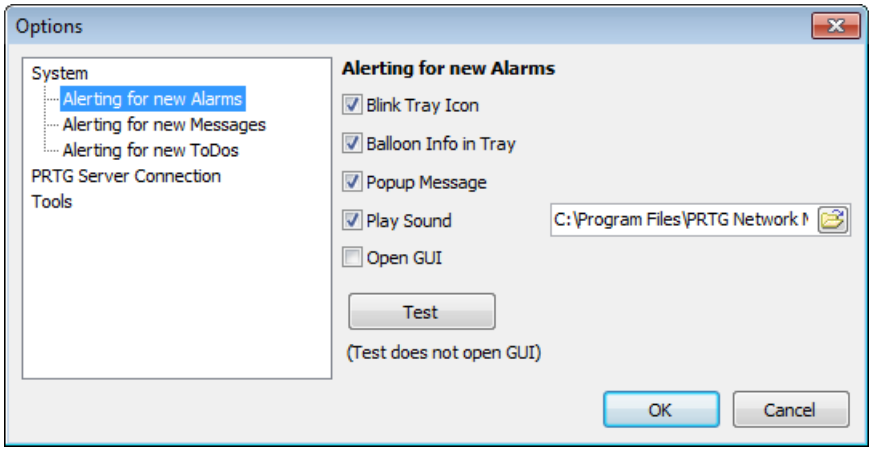
Language

- Choose the language for this program from the drop down menu. Default is **English**. Depending on your installation, you may be able to choose other languages here.
- This setting will influence the language of the Windows GUI only.

System—Alerting

You can define what the Windows GUI will do in case of new **Alarms**, **Messages**, or **ToDos**. The settings are the same for all of these three cases, but you can individually define them for each case. On the left side, please select either **Alerting for new Alarms**, **Alerting for new Messages**, or **Alerting for new ToDos** and define the settings as follows.

Note: All alerting options only take effect when the **Show in Tray** option is enabled in the system 913 settings above; if the tray icon is disabled, there will be no alerting from the Windows GUI.



Windows GUI System Settings for Alerting

Blink Tray Icon

- The tray icon will blink if there are new items to be alerted for.
- You can additionally set the **Clear Tray Blink Notification automatically** option in the system 913 settings above.

Balloon Info in Tray

- Show a balloon info next to the PRTG tray icon if there are new items to be alerted for.

© 2011 Paessler AG

Popup Message

- Show a popup message window if there are new items to be alerted for.
- *Note:* The popup window will be always on top until it's closed.

Play Sound

- Play an audible notification if there are new items to be alerted for.
- There is a default sound defined. To change it, please click on the folder symbol and select any standard WAV file from your hard disk drive. PRTG already comes with a small set of sounds you can choose from.
- *Note:* The sound file will be played only on the computer running the Windows GUI.

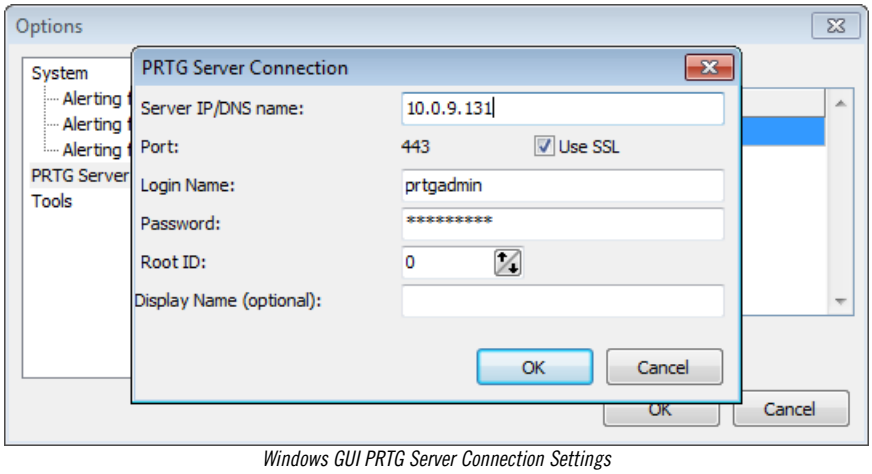
Open GUI

- Open the Windows GUI if there are new items to be alerted for.

PRTG Server Connection

The Windows GUI connects to the web server running with every PRTG core server installation. It supports saving the configuration for a connection to one or more PRTG web servers. In a full PRTG installation, there is already a connection predefined. *Note:* For a successful connection, the program versions of Windows GUI and PRTG core server have to match.

Please click the **Add** button to add a new server connection configuration, or choose an existing **Server** from the list and click the **Edit** button to change the settings. Use the **Delete** button to remove an entry from the list. When opening the Windows GUI, it will automatically re-establish the connection used previously.



Windows GUI PRTG Server Connection Settings

Server IP/DNS name

- Enter the IP address or DNS name of the PRTG web server the Windows GUI will connect to.
- This is the same address or name as defined in the web server settings for the core server. For detailed information please see PRTG Server Administrator 955 (**Web Server**) section. Please make sure that the set values match.

- Please make sure that the server is reachable (especially when using Network Address Translation (NAT)) and no firewall settings are blocking the connection.

Port

- Enter the port on which the PRTG web server is running.
- This is the same port as defined in the web server settings for the core server. For detailed information please see PRTG Server Administrator 955 (**Web Server**) section. Please make sure that the set values match.
- Please make sure that the server is reachable (especially when using Network Address Translation (NAT)) and no firewall settings are blocking the connection.

Login Name

- Enter the login name that will be used to login to the web server.
- This can be the administrator login or the login of another PRTG user.
- In a new installation, the login name is **prtgadmin** by default.
- For detailed information about user accounts please see System Administration—User Accounts 884 section.

Password

- Enter the password for the login name entered above.
- In a new installation, the password is **prtgadmin** by default.

Root ID

- Enter the ID of the object that will be considered the root of the device tree.
- Default value is **0**, which is the Root group of your configuration.
- If you enter an other object's ID here, the device tree will start at this object, only showing all other objects below in the hierarchy.
- This is useful to only view a part of the device tree, which is loaded much faster.
- You can create several connections that only differ in the **Root ID** value in order to quickly switch between different views within your configuration, choosing different connections from the **File** Windows menu 919.

Display Name (optional)

- Optionally enter a name that will be displayed in the **Server** list.
- If you leave this field blank, the **Server IP/DNS name** setting will be displayed there.

Click the **OK** button to save your settings.

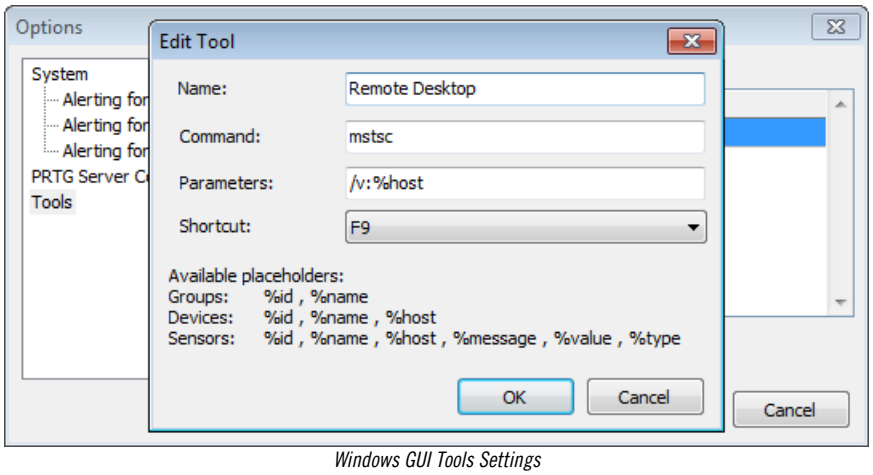
Tools

In the **Tools** settings you can define commands that will be available in the Windows Menu 919 and context menu 922 of groups, devices, and sensors. A command to initiate a remote desktop connection is already predefined.

Note: In order for the tool function to work with your Windows version, you may need to run the Windows GUI as administrator.

© 2011 Paessler AG

Please click the **Add** button to add a new command, or choose an existing one from the list and click the **Edit** button to change the settings. Use the **Delete** button to remove an entry from the list.



Windows GUI Tools Settings

Name

- Enter a custom name for your command as it will show up in the context menu.

Command

- Enter the command you want to execute on the local machine.
- This can be, for example the name of a program or script, with or without path, according to your system's configuration.

Parameters

- Enter the parameters with which the command will be called.
- You can use the placeholders (variables) shown in the window. Other placeholders are *not* possible. During runtime, these placeholders will be replaced by the respective values set for the object you have selected. For example, the *%id* placeholder will be replaced by the ID of a group, a device, or a sensor, depending on which object you're executing the command for.

Parameters—Available placeholders

The following placeholders (variables) are available in the Windows GUI.

Placeholder	Available For Groups	Available For Devices	Available For Sensors	Will Be Resolved To
%id	X	X	X	The object's **ID** as shown in brackets behind the name
%name	X	X	X	The object's **Name** value.
%host	—	X	X	The sensor's or device's **IP Address/DNS Name** value
%message	—	—	X	The sensor's **Last Message** value
%value	—	—	X	The sensor's **Last Result** value
%type	—	—	X	The sensor's **Type** value

If a placeholder is used in combination with an object it is not available for, it will simply not be resolved, but the placeholder itself will be returned.

Note: To see the output of all placeholders for different objects you can create a simple test tool that displays the output in a command line window. Just create a tool with the command **cmd** and the following content in the **Parameters** field:

```
/K echo.id: %id && echo.name: %name
       && echo.host: %host && echo.message: %message
       && echo.value: %value && echo.type: %type
```

Then, click an object in the device tree and run the tool from the **Tools** option in the menu (either Windows 919 or context menu 922).

Shortcut

- Select a key shortcut for the command. Choose an **F**-Key from the list or select **None** to not use a key.

Select External Browser

With this settings you can define which browser will be opened when you select a command which requires opening an external browser window, for example when calling **View | Open this object in** *Web Browser*. You can only select browsers installed on the system running the Windows GUI; other browser options are disabled. By default, the system's default browser is opened. To change this behavior, choose between:

- **Use system default browser**
- **Use IE**
- **Use Firefox**
- **Use Chrome**
- **Use Safari**

© 2011 Paessler AG

8.5 Windows Menu Structure

The Windows menu has four main menu items:

- File 919
- Edit 919
- View 921
- Help 921

File

- **Select PRTG Server ›**
  If you configured connections to several PRTG core servers, you can select one here. *Hover* to see all available connections and choose one. The Windows GUI will instantly try to connect.

- **Options & Server Settings...**
  Open the dialog to set options and to configure one or more PRTG core server connections. For detailed instructions, please see Options and Server Settings 913.

- **Close / Exit**
  This menu item appears as either **Close** or **Exit**, depending on whether the tray icon is enabled or disabled in the Options and Server Settings 913. **Close** will close the Windows GUI, but alerting will still be available via the tray icon. You can also double click on the tray icon to re-open the Windows GUI. **Exit** will completely shut down the Windows GUI. This option is only available if the tray icon is not running.

Edit

The content of the **Edit** menu varies, depending on whether and which objects are selected within the Devices 900, Sensors 904, or Alarms 906 tab.

Note: Some of the options will open the Ajax web interface.

When you click on one of these items, a new window or tab of your system's default browser will open and PRTG will automatically login and redirect you to the respective web page. If your browser displays a certificate warning, please find more information in the Login 93 section (**Confirm Certificate for Https Connection**).

- **Add Group...**
  This option is available only when a probe or group (*not* the **Root** group) is selected. This will open the Ajax web interface which guides you through adding a new group to the selected probe or group. For detailed instructions, please see Add a Group 157.

- **Add Device...**
  This option is available only when a probe or group (*not* the **Root** group) is selected. This will open the Ajax web interface which guides you through adding a new device to the selected probe or group. For detailed instructions, please see Add a Device 160.

- **Add Sensor...**
  This option is available only when a device is selected. This will open the Ajax web interface which guides you through adding a new sensor to the selected device. For detailed instructions, please see Add a Sensor 165.

- **Run Auto-Discovery**
  This option is available only when a device is selected. If you select this option, an automatic search is started, adding new sensors to the selected device. The search is running in the background. If found, you will see new sensors after a few minutes automatically. For more information, please see Auto-Discovery 146 (**Run Auto-Discovery Now**).

- **Create Device Template...**
  This option is available only when a device is selected. This will open the Ajax web interface which guides you through creating a device template; this will then be available in auto-discovery 145. For detailed instructions, please see Create Device Template 815.

- **Check Now**
  For all selected objects from the device tree (use the *Ctrl* key to select multiple objects), perform an immediate scan. This will poll all selected devices and query new data for all sensors on them. If you choose this option for a probe or a group, data for all sensors in the object hierarchy 79 underneath will be queried.

- **Acknowledge Alarm...**
  This option is available only when a sensor in a **Down** or **Down (Partial)** status is selected. For details on how to acknowledge an alarm, please see Alarms 906 section.

- **Delete**
  This will delete the selected object(s). You will be asked for confirmation before anything is actually deleted.

- **Clone...**
  This option is available only when a single group, device, or sensor is selected. This will open the Ajax web interface which guides you through cloning the selected object. For detailed instructions, please see Clone Object 817.

- **Pause ›**
  For all selected objects from the device tree (use the *Ctrl* key to select multiple objects), you can pause and resume monitoring, or set a sensor to error for testing purposes. *Hover* to see available options. You can choose between: Pause **Indefinitely**, **Resume** from pause, pause **For 5 Minutes**, **For 15 Minutes**, **For 1 Hour**, **For 3 Hours**, **For 1 Day**, or **Set Sensor to Error**. The last option only takes effect with a sensor is chosen.

- **Rename...**
  Rename the selected object. A popup will appear. Please enter a new name and confirm with the **OK** button.

- **Drag & Drop Sorting**
  In order to use the option to sort all objects in the device tree via drag and drop, please enable this option. By default, this option is disabled to avoid accidental moves of objects.

© 2011 Paessler AG

- **Tools ›**
  Call a tool command. All placeholders (variables) configured in a tool command will be resolved for the currently selected object. *Hover* to see all available tools configured in your Options and Server Settings 916 (**Tools**). By default, a **Remote Desktop** tool is pre-configured which tries to initiate a remote desktop connection to the IP address or DNS name of the selected object (this will usually work for devices, of course).

  For devices, additional options are available. They allow you to connect to the **Service URL** value defined in the device's settings 902, or open the **IP address/DNS name** of the device via the protocols *HTTP*, *HTTPS*, and *FTP*. For each of these functions, your system's default programs will be used. Usually, this is your browser.

  Note: In order for the tool function to work with your Windows version, you may need to run the Windows GUI as administrator.

View

- **Refresh**
  This will immediately query data for the current screen from the PRTG core server, just as the automatic refresh does, which can be configured in the Options and Server Settings 913.

- **Open Web GUI...**
  This will open the start page of the Ajax web interface in the external browser. The default browser can be set in the Options and Server Settings 918.

- **Large Single Graph**
  Change the view in Devices 900 menu tab to large single graphs. This will display live graphs, and graphs for three other time spans, in different tabs.

- **Small Multiple Graphs**
  Change the view in Devices 900 menu tab to multiple small graphs. This will display live graphs, and graphs for three other time spans. This will display all graphs in one tab.

- **Open this object in** *Web Browser*
  This will open the currently selected object in the Ajax web interface. This option is not available if multiple objects are selected. The default browser can be set in the Options and Server Settings 918.

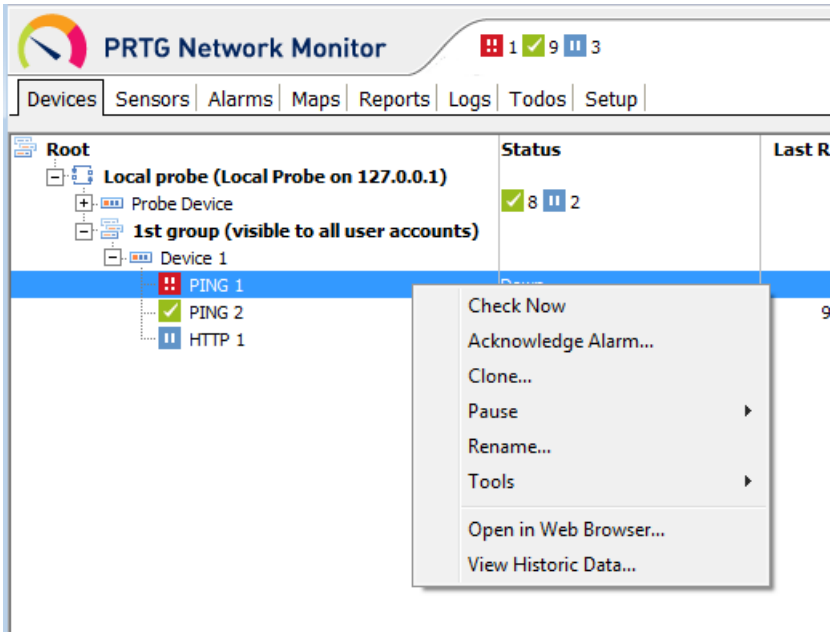
- **View Historic Data...**
  This option is available only when a single sensor is selected. This will open the Ajax web interface which guides you through the process of viewing historic data. For detailed instructions, please see Historic Data Reports 107 (**Menu**).

Help

This menu provides web site links to the HTML manual, the Paessler Knowledge Base, the Paessler website, and displays program information when you select **About...**.

8.6 Context Menus

For every object in the Windows GUI, there are context menus available which appear when you right-click on object. These context menus vary depending on the selected object and always contain a subset of the options available in the Windows menu. For detailed explanations, please see Windows Menu Structure 919.



Example of a Context Menu in Windows GUI

© 2011 Paessler AG

8.7 Shortcuts Overview

The following shortcut keys are available in the Windows GUI:

Alt+X: File | Close *or* Exit
With Windows tray icon enabled, this will be **Close**; otherwise **Exit**.

Ctrl+C: Edit | Check Now

Ctrl+P: Edit | Pause | Indefinitely

Ctrl+R: Edit | Pause | Resume

Ctrl+L: View | Large Single Graph

Ctrl+S: View | Small Multi Graphs

Ctrl+H: View | Hide Googlemap

F5: View | Refresh

F6: [Context Menu] | Tools | *Custom tool command, if available*

F7: [Context Menu] | Tools | *Custom tool command, if available*

F8: [Context Menu] | Tools | *Custom tool command, if available*

F9: [Context Menu] | Tools | *Custom tool command* (default: **Remote Desktop**)

F10: [Context Menu] | Tools | *Custom tool command, if available*

F11: [Context Menu] | Tools | *Custom tool command, if available*

F12: [Context Menu] | Tools | *Custom tool command, if available*

© 2011 Paessler AG

Part IX

Other User Interfaces

9 Other User Interfaces

This chapter introduces other available user interfaces, mainly optimized for mobile access. Read more in the following sections.

Other User Interfaces—Topics

- HTML GUI (Low bandwidth) 927
- iPhone Interface 930

Related Topics

- Ajax Web Interface—Basic Procedures 92
- Ajax Web Interface—Device and Sensor Setup 144
- Ajax Web Interface—Advanced Procedures 806
- Windows GUI 894

© 2011 Paessler AG

9.1 HTML GUI (Low bandwidth)

The HTML GUI is slim interface to view your monitoring results while on the go. It is optimized for both small screens and low bandwidth usage in order to provide an easy and fast access to your PRTG core server when connecting with mobile devices. You can view sensor lists, data tables, and graphs with live data.

HTML GUI on Different Mobile Devices

Compared to the Ajax GUI 92, this interface comes with limited functionality and is primarily provided as an addition. Nevertheless, you can acknowledge alarms, pause or resume monitoring, and interactively view sensors and other lists.

Loading the Web Interface

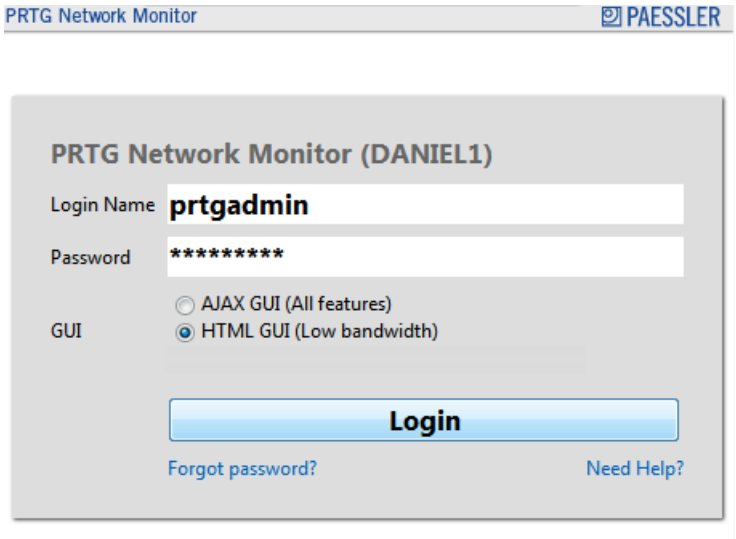
Make sure your PRTG core installation is accessible via the Internet. In your mobile device, enter the IP address or URL of the system PRTG is installed on. When using a cluster, you can connect to any node accessible.

Confirm Certificate for Https Connection

In a standard setup, the connection to the web interface is SSL-encrypted, using a certificate that is automatically installed with PRTG. Although the connection is securely encrypted, it is not a "trusted" certificate issued by a known entity. That's why usually your mobile browser will show a certificate warning that can look different with every system. Please confirm the certificate in order to proceed to the login screen.

Login Screen

After loading the web interface, the login screen is shown.



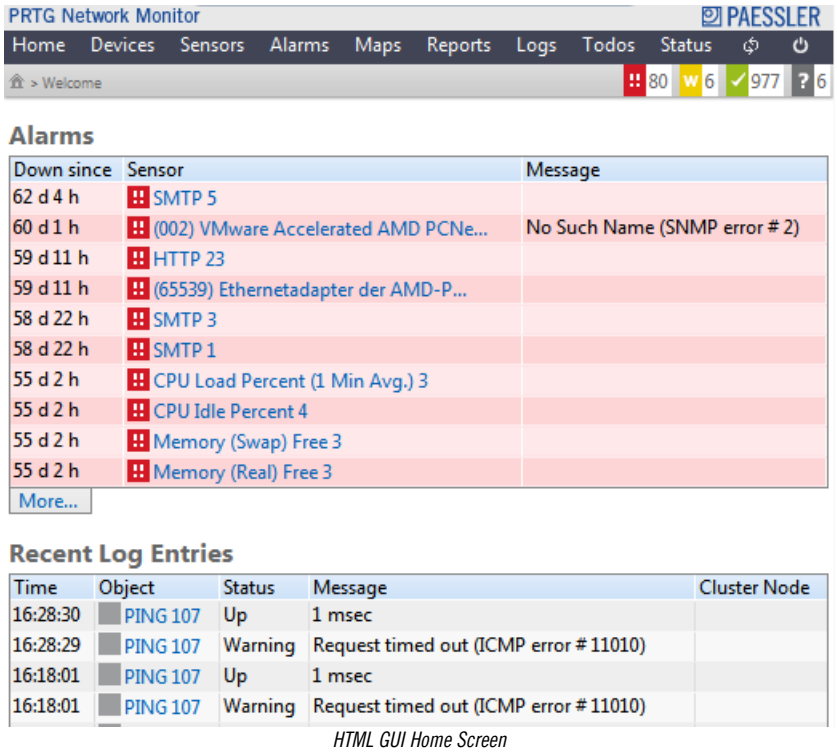
HTML GUI Login

Enter your credentials, choose the **HTML GUI (Low bandwidth)** option, and click on **Login**. For detailed information about different credentials, please see the Login 94 section for the Ajax GUI.

General Layout

The home screen of the HTML GUI shows the excerpt of the current **Alarms** list, as well as the last **Recent Log Entries**. You can click on sensors to view details, or use the main menu to load other views of your setup.

© 2011 Paessler AG


PRTG Network Monitor
PAESSLER
Home Devices Sensors Alarms Maps Reports Logs Todos Status
> Welcome
80 6 977 6
Alarms
Down since Sensor Message
62 d 4 h SMTP 5
60 d 1 h (002) VMware Accelerated AMD PCNe... No Such Name (SNMP error # 2)
59 d 11 h HTTP 23
59 d 11 h (65539) Ethernetadapter der AMD-P...
58 d 22 h SMTP 3
58 d 22 h SMTP 1
55 d 2 h CPU Load Percent (1 Min Avg.) 3
55 d 2 h CPU Idle Percent 4
55 d 2 h Memory (Swap) Free 3
55 d 2 h Memory (Real) Free 3
More...
Recent Log Entries
Time Object Status Message Cluster Node
16:28:30 PING 107 Up 1 msec
16:28:29 PING 107 Warning Request timed out (ICMP error # 11010)
16:18:01 PING 107 Up 1 msec
16:18:01 PING 107 Warning Request timed out (ICMP error # 11010)

HTML GUI Home Screen

Click on the **Devices** entry in the main menu to view the device tree, or choose one of the other options.

Using the HTML GUI

The device tree and lists of sensors, alarms, logs, and ToDos are available as usual, but it a view optimized for mobile screens. Also, monitoring data for all objects can be viewed. This section will not explain the GUI in detail, as the concepts are the same as throughout the Ajax web interface 92. In the following, find a list with the main differences, compared to the full Ajax interface:

- There are no context menus available, but actions such as acknowledge an alarm, scan now, pause, etc. can be initiated directly on an objects detail page, using the respective buttons.
- All filter options in lists are displayed "flat", using direct links instead of cascading menus and tabs.
- Reports and Maps are accessible in view only mode.
- You cannot edit system settings.
- From within the HTML GUI, you can switch to the Ajax web interface any time by using the **Go To AJAX interface** link.

We're sure you'll just need a few minutes to get familiar with this interface. Have fun monitoring while on the go!

9.2 Smart Phone Apps

There are apps for the iPhone and for Android devices, with which you can connect to your PRTG installation while on the go. Use them as an alternative to the HTML GUI 927 interface.

iOS: iPRTG

iPRTG is the iApp for PRTG Network Monitor. Use it on the iPhone, iPad, and iPod Touch.

iPRTG Screenshots

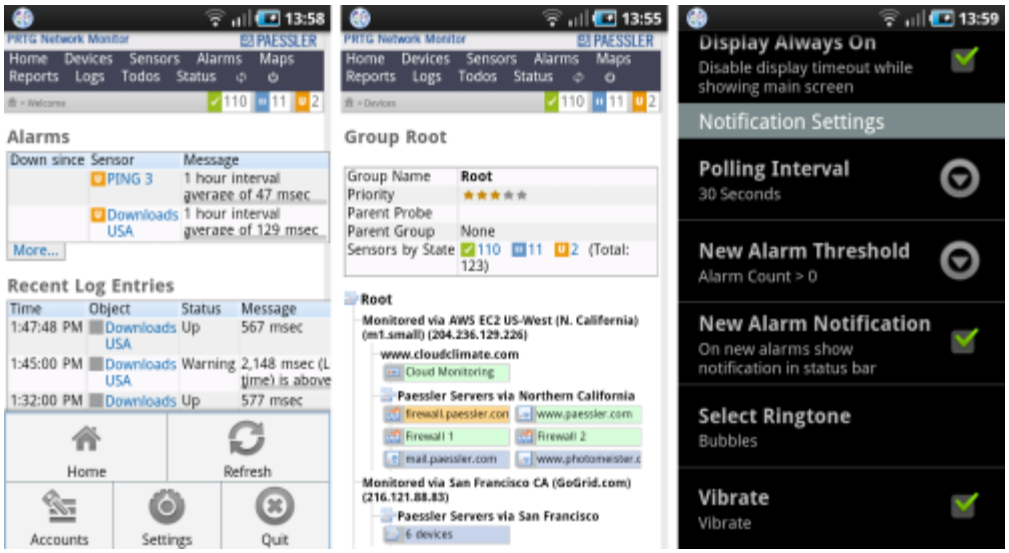
Don't let monitoring your network tie you to your desk! With iPRTG your network monitor is where your iPhone is. iPRTG is the iPhone App for network administrators using the PRTG Network Monitor software to monitor and administrate their network. iPRTG is the one and only clear and simple viewer for the entire network monitoring environment. Your iPhone requests the monitoring data directly from your PRTG server and displays it in an 'iPhonic' way.

In order to use iPRTG, your core server must be reachable from the Internet. You can view monitoring data and perform certain actions, such as acknowledge alarms, pause or resume monitoring, etc.

Android: PRTGdroid

PRTGdroid is the Android app for PRTG Network Monitor. Use it on your phone or tab.

© 2011 Paessler AG



PRTGdroid Screenshots

The features include:

- Multiple accounts support to query different server/login combinations. Switch easily between different accounts to quickly view monitoring data of several installations and/or accounts.
- The app can check all accounts, or only specific ones, automatically in the configured polling interval and notify you in your device's status bar whenever there are alarms for one of them.
- Configure when you want to be notified: Alarms > 0 or when alarms count raised since last check. Configure notifications via the system status bar with ringtone and/or vibration (triggered for new notifications).

In order to use PRTGdroid, your core server must be reachable from the Internet. The app embeds PRTG's 'Mini HTML' interface to display monitoring data. All features of this browser interface are available: You can acknowledge alarms, pause and resume sensors, view geo maps, change the zoom factor, etc.

More

More information and a video about iPRTG

- http://www.paessler.com/iprtg

More information about PRTGdroid

- http://www.paessler.com/androidapp

Part X

Sensor Technologies

10 Sensor Technologies

This chapter introduces different technologies that PRTG uses for monitoring, in order to give you a little more background information. Please read more in the following sections.

Sensor Technologies—Topics

- Monitoring via SNMP 935
- Monitoring via WMI 938
- Monitoring Bandwidth via Packet Sniffing 940
- Monitoring Bandwidth via Flows 942
- Bandwidth Monitoring Comparison 944
- Monitoring Quality of Service 947
- Monitoring Email Round Trip 951

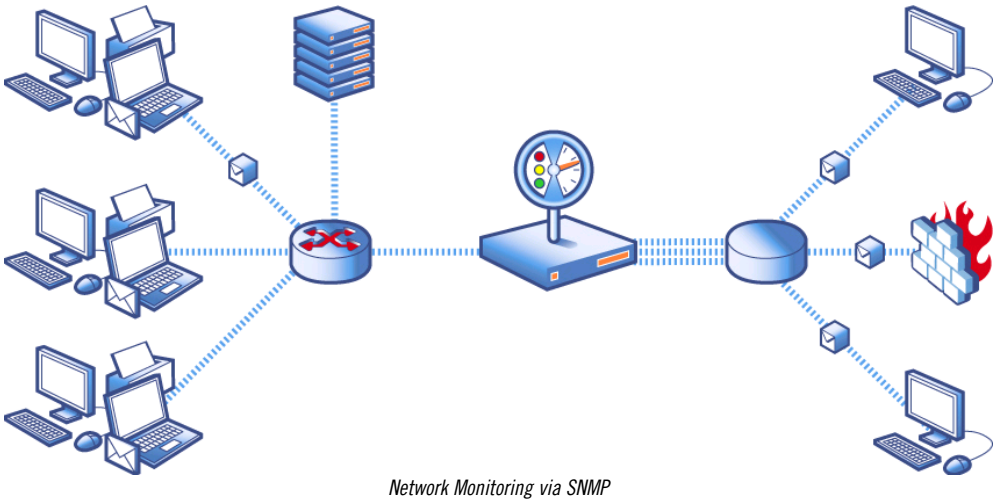
© 2011 Paessler AG

10.1 Monitoring via SNMP

Monitoring via Simple Network Management Protocol (SNMP) is the most basic method of gathering bandwidth and network usage data.

How SNMP Monitoring Works

SNMP can be used to monitor bandwidth usage of routers and switches on a port-by-port basis, as well as device readings such as memory, CPU load, etc. The queried devices must support SNMP.



Network Monitoring via SNMP

When this technology is used, PRTG sends small data packets to devices, for example, querying routers, switches, and servers for the traffic counters of each port. These are triggering reply packets from the device. Compared to PRTG's other bandwidth monitoring techologies via flows, packet sniffing, or WMI, the SNMP option creates the least CPU and network load.

Reasons to Choose SNMP Monitoring

SNMP is the most commonly used method mainly because it is easy to set up and requires minimal bandwidth and CPU cycles. If your network devices support SNMP and/or if you want to monitor large networks with several hundred or thousands of sensors, we recommend you start with SNMP. Besides network usage monitoring, another well-known feature of SNMP is the ability to also watch other network parameters such as CPU load, disk usage, temperature, as well monitoring many other readings, depending on the queried device.

SNMP Network Issues

In order to use Simple Network Management Protocol (SNMP) for monitoring purposes, it is imperative that UDP packets are allowed to travel from the machine running PRTG to the device you want to monitor and back, which is usually the case in LANs and Intranets. For connections across the Internet, to a Demilitarized Zone (DMZ), or for Wide Area Network (WAN) connections, some changes to the traversed firewalls may be necessary. Keep in mind that SNMP V1 and V2c are not secure protocols and should not be used across the Internet or insecure data connections. Only SNMP version 3 supports encryption.

© 2011 Paessler AG

Understanding SNMP Sensors

To better understand and set up SNMP sensors, you may want to learn more about the principle of Object Identifiers (OID) and Management Information Base (MIB). For more information about this, please refer to the Knowledge Base article in the More 937 section below.

For an overview and details about all SNMP sensors, please see the List of Available Sensor Types 204 section.

SNMP Versions

PRTG supports three versions of the SNMP protocol: Version 1, version 2c, and version 3.

SNMP Version 1

This is the oldest and most basic version of SNMP.

- Pro: Supported by most SNMP-compatible devices; simple to set up.
- Contra: Limited security as it only uses a simple password (*community string*) and data is sent in clear text (unencrypted). It should therefore only be used inside LANs behind firewalls, not in WANs; only supports 32-bit counters which is not enough for high-load (gigabits/second) bandwidth monitoring.

SNMP Version 2c

This version adds 64-bit counters.

- Pro: Supports 64-bit counters to monitor bandwidth usage in networks with gigabits/second loads.
- Contra: Limited security (same as with SNMP V1).

SNMP Version 3

This version adds authentication and encryption to SNMP.

- Pro: Offers user accounts and authentication for multiple users and optional data packet encryption, increasing available security; plus all advantages of Version 2c.
- Contra: Difficult to configure. Not suitable for large networks (see below for more information).

It is important to know that if you select an SNMP version which is not supported by the server or device you want to monitor, you will receive an error message. Unfortunately, in most cases, these error messages do not explicitly mention the possibility that you could be using the incorrect SNMP version. These messages provide minimum information only, such as *cannot connect* or similar. Similar error occur when community strings, usernames, or passwords don't match.

© 2011 Paessler AG

SNMP Overload and Limitations of the SNMP System

SNMP V1 and V2 scale directly with the performance of the hardware and the speed of the network. In our labs we were able to monitor 30,000 SNMP V1 sensors at a 60 second interval with one PRTG server (core and local probe) plus two remote probes with 10,000 sensors each.

However, SNMP V3 has software dependent performance limitations due to the SSL encryption. Because of internal limitations you can only monitor a limited number of sensors per second using SNMP V3. The limit is somewhere between 1 and 50 sensors per second, depending on the SNMP latency of your network. This means that using an interval of 60 seconds you are limited to between 60 and 3,000 SNMP V3 sensors for each probe. If you experience an increased *Probe Interval Delay SNMP* or *Probe Open Requests* channels of the **Core/Probe Health** 233 sensor (values above 0 % indicate that the SNMP requests cannot be performed at the desired interval) you need to distribute the load over multiple probes. SNMP V1 and V2 do not have this limitation.

If you run into SNMP overload problems you have three options:

- Increase the monitoring interval of the SNMP V3 sensors.
- Distribute the SNMP V3 sensors over two or more probes.
- Switch to SNMP V1 or V2 if you can go without encryption.

What is the SNMP Community String?

The SNMP *Community String* is similar to a user ID or password that allows access to a router's or other device's statistics. PRTG Network Monitor sends the community string along with all SNMP requests. If the correct community string is provided, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond.

Note: SNMP community strings are only used by devices that support SNMP V1 and SNMP V2c protocols. SNMP V3 uses safer username/password authentication, along with an encryption key.

By convention, most SNMP V1/V2c equipment ships with a read-only community string set to the value **public**. It is standard practice for network managers to change all the community strings to customized values during device setup.

More

Tools: Paessler MIB Importer and SNMP Tester

- http://www.paessler.com/tools/

Paessler White Papers: *Introducing SNMP* and *Putting SNMP into Practice*

- http://www.paessler.com/company/press/whitepapers/introducing_snmp

10.2 Monitoring via WMI

Windows Management Instrumentation (WMI) is Microsoft's base technology for monitoring and managing Windows based systems.

How WMI Works

WMI allows accessing data of many Windows configuration parameters, as well as current system status values. Access can be local or remote via a network connection. WMI is based on *COM* and *DCOM* and is integrated in Windows 2000, XP, 2003, Vista, 2008, and Windows 7 (add-ons are available for Windows 9x and NT4). PRTG officially supports WMI for Windows XP or later.

In order to monitor remote machines, PRTG's WMI sensor needs Active Directory account credentials to have access to the WMI interface. You can enter these credentials in PRTG for the parent device or group, or in the **Root** 166 group. The sensor will then inherit these settings.

For an overview and details about all WMI sensors, please see the **List of Available Sensor Types** 204 section.

Limitations of WMI on Windows Vista and Windows Server 2008 R1

You should be aware that performance of WMI based monitoring is drastically limited when the monitoring station or the monitored client runs on Windows Vista or Windows Server 2008 R1. When it comes to network monitoring via WMI, Windows XP and Windows 2003 are up to 70 times faster than Windows 2008 or Vista.

Note: These are not limitations of PRTG, but arise from the WMI functionality built into the Windows operating systems mentioned.

The results of our tests are:

- On Windows XP/Windows 2003/Windows 7/Windows 2008 R2 you can run about 10,000 WMI sensors with one minute interval under optimal conditions (such as running the core and the target systems exclusively under Windows 2003 and being located within the same LAN segment). Actual performance can be significantly less depending on network topology and WMI health of the target systems - we have seen configurations that could not go beyond 500 sensors (and even less).
- On Windows Vista/Windows 2008 R1 you can run about 300 WMI sensors with one minute interval.
- The more Windows Vista/Windows 2008/Windows 7 client systems you have in your network the more WMI monitoring performance will be affected.
- System performance (CPU, memory etc.) of virtualization does not strongly affect WMI monitoring performance.

If you want to use WMI for network monitoring of more than 20 or 30 systems, please consider the following rules:

- Do not use Windows Vista or Windows 2008 R1 as monitoring stations for WMI-based network monitoring.
- If possible use Windows 2003 R2 Server for WMI based network monitoring (followed by XP and Windows 7/2008 R2).

© 2011 Paessler AG

- If you cannot run PRTG on Windows XP/Windows 2003 consider setting up a remote probe with XP for the WMI monitoring. (You still get far better WMI monitoring performance with a remote probe on a virtual machine running Windows XP or Windows 2003 than on any bare metal system running Windows Vista/Windows 2008 R1.)
- Consider switching to SNMP-based monitoring for large networks. Using SNMP you can easily monitor 10 times as many nodes as with WMI (on the same hardware).

More

Knowledge Base: General introduction to WMI and PRTG
- http://www.paessler.com/knowledgebase/en/topic/1043

Tool: Paessler WMI Tester. A useful freeware tool to test WMI connections. Tests the accessibility of WMI (Windows Management Instrumentation) counters in a quick and easy manner.
- http://www.paessler.com/tools/wmitester

CEO's Blog: Don't Use Windows Vista And Windows 2008 R1 for Network Monitoring via WMI!
- http://www.paessler.com/blog/2010/09/22/

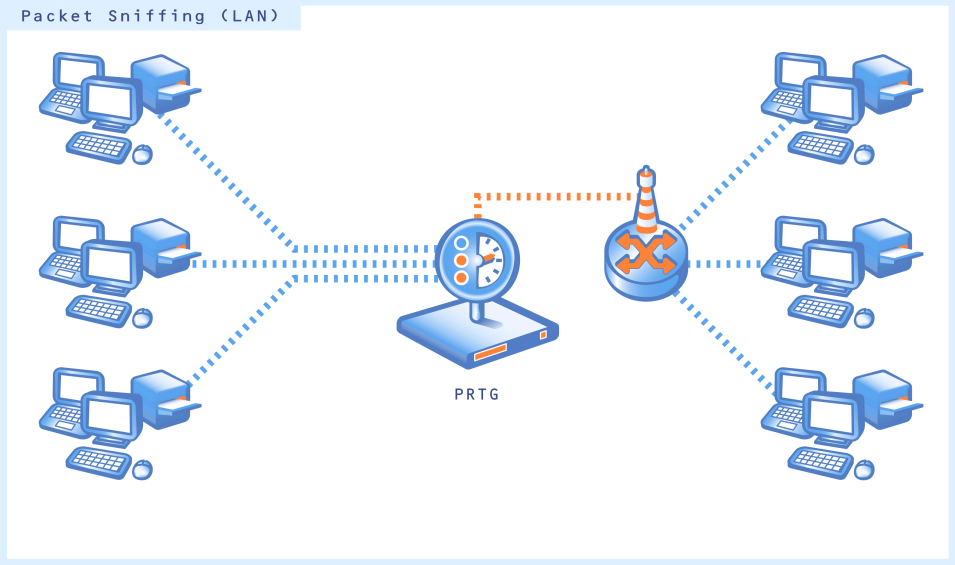
10.3 Monitoring Bandwidth via Packet Sniffing

Packet Sniffing should come into consideration if your network device(s) do not support SNMP or xFlow to measure bandwidth usage and if you need to differentiate the bandwidth usage by network protocol and/or IP addresses.

Note: Packet Sniffer Sensors support Toplists (Top Talkers, Top Connections, etc.), see Toplists 807 section.

How Packet Sniffing works

If you need to know what applications or IP addresses are causing the traffic in your network, you can use a packet sniffer. This will look at every single data packet traveling through your network for accounting purposes.



Monitoring with PRTG via Packet Sniffer Sensors

PRTG can analyze the packets passing the network card of a PC or it can be connected to the so-called monitoring port of a switch. In order to calculate bandwidth usage, PRTG inspects all network data packets either passing the PC's network card (shown on the left side) or the data packets sent by a monitoring port of a switch (right side) with its built-in packet sniffer. Using remote probes you can set up packet sniffers anywhere in your network (see Add Remote Probe 986 section).

Comparing the four bandwidth monitoring technologies provided by PRTG (SNMP, WMI, xFlow and packet sniffer) this one creates the most CPU and network load and should thus only be used in small to medium networks, on dedicated computers for larger networks or for individual computers.

© 2011 Paessler AG

Reasons To Choose Packet Sniffing

It is important to understand that the packet sniffer can only access and inspect data packets that actually flow through the network interface(s) of the machine running the PRTG probe software. This is fine if you only want to monitor the traffic of this machine (e.g. your web server). In switched networks, only the traffic for a specific machine is sent to each machine's network card, so PRTG can usually not discern the traffic of the other machines in the network.

If you also want to monitor the traffic of other devices in your network, you must use a switch that offers a "monitoring port" or "port mirroring" configuration (Cisco calls it "SPAN"). In this case the switch sends a copy to the monitoring port of all data packets traveling through the switch. As soon as you connect one of the PRTG probe system's network cards to the switch's monitoring port, PRTG is able to analyze the complete traffic that passes through the switch.

Another option is to set up the PC running PRTG as the gateway for all other computers in the network.

Set Up Packet Sniffer Sensors

Find details on how to set up the different flow sensors in the following sections:

- Packet Sniffer (Content) Sensor 434
- Packet Sniffer (Header) Sensor 446
- Packet Sniffer (Custom) Sensor 440

Header Based vs. Content Based Packet Sniffing

PRTG provides two base technologies for packet sniffing:

- **Header based**: PRTG looks at the IPs and ports of source and destination to assess the protocol. This is very fast but, at times, not very accurate. For example it is not possible to identify HTTP traffic on ports other than 80, 8080 and 443 as HTTP.

- **Content based**: PRTG captures the TCP packets, reassembles the data streams and then analyzes the content of the data using an internal set of rules to identify the type of traffic. This is quite accurate (e.g. HTTP traffic on any port number is accounted for as HTTP) but requires much more CPU and memory resources, especially when a lot of traffic passes the network card.

To summarize, header based sniffing is much faster but the accounting is less reliable (e.g. HTTP packets on non-standard ports are not accounted as HTTP traffic). Content based sniffing is quite accurate, but creates more CPU load.

More

Tool: Paessler Card Packet Counter: Shows short term statistics about the network data packets passing a local network card.
- http://www.paessler.com/tools/

10.4 Monitoring Bandwidth via Flows

Using Flow protocols you can monitor the bandwidth usage of all packets going through a device. In PRTG, you can view Toplists 807 for all xFlow sensors.

How xFlow Monitoring works

You can measure bandwidth usage *by IP address* or *by application* in a network, using one of the xFlow protocols. They are the best choice especially for networks with high traffic (connections with 100s of megabit or gigabits). For xFlow monitoring the router gathers bandwidth usage data (*flows*), aggregates them and sends information about these flows to PRTG using UDP packets. When sampling is used (mandatory for sFlow) only information about every n-th packet is sent to PRTG which reduces CPU load a lot. Because the switch already performs a pre-aggregation of traffic data, the flow of data to PRTG is much smaller than the monitored traffic. This makes xFlow the ideal option for high traffic networks that need to differentiate the bandwidth usage by network protocol and/or IP addresses.

NetFlow Monitoring

The NetFlow protocol is mainly used by Cisco devices. Once configured, the router sends for each data flow a NetFlow packet to the monitoring system running on a PRTG probe. There the data can be filtered and evaluated. There are different NetFlow sensors available: The basic ones offer predefined channel definitions, the custom variants enable you to define your own channels.

The advantage of using NetFlow:

- Generates little CPU load on the router itself (according to Cisco 10,000 active flows create about 7% additional CPU load; 45,000 active flows account for about 20% additional CPU load).
- Generates less CPU load on the PRTG core system, compared to packet sniffer sensors.

Note: You must enable NetFlow export on the device you want to monitor. The device must send a flow data stream to the IP address of the PRTG probe system on which the NetFlow sensor is set up. Use a separate UDP port for every device. Juniper **jFlow** monitoring is reported to work as well, using NetFlow v5 sensors.

sFlow Monitoring

sFlow works similar to NetFlow monitoring. The router sends data flow packets to the monitoring system running on a PRTG probe. The most obvious difference between the two flow protocols: With sFlow, not all of the traffic is analysed, but only every n-th packet. It is like having a river of traffic and you take a cup of water out of it ever so often and analyze it.

The advantage is clear: There is less data to analyze, there is less CPU load needed and less monitoring traffic is generated. Yet you can get a good insight into your network's bandwidth usage. *Note:* Currently, PRTG supports sFlow version 5.

Set Up Flow Sensors

Find details on how to set up the different flow sensors in the following sections:

- NetFlow V5 Sensor 394

© 2011 Paessler AG

- NetFlow V5 (Custom) Sensor 400
- NetFlow V9 Sensor 406
- NetFlow V9 (Custom) Sensor 412
- sFlow Sensor 504
- sFlow (Custom) Sensor 510
- jFlow V5 Sensor 357
- jFlow V5 (Custom) Sensor 363

Limitations

On a powerful 2008 PC (Dual Core, 2.5 Ghz), you can process about 100,000 flows per second for one xFlow stream. Using sampling the number of actual flows can be much higher. When using complex filters, the value can be much lower. For example, with a router sending about 2,000 flows/second (which corresponds to mixed traffic at gigabit/sec level without sampling) you can expect to configure up to 50 NetFlow sensors operating properly. PRTG internally monitors its own NetFlow processing, and you will see a decreased values in the Core/Probe Health 233 sensor's *Health* channel as soon as NetFlow packets are not processed due to an overload (you find this sensor on the Local Probe device).

If you experience an overload please consider using sampling or setting up multiple probes and distribute the NetFlow streams to them. We do not recommend adding more than 400 NetFlow sensors per PRTG probe.

More

Knowledge Base: Can I add custom channels to standard Packet Sniffer and NetFlow sensors?
- http://www.paessler.com/knowledgebase/en/topic/2143

Knowledge Base: What filter rules can be used for custom Packet Sniffing or xFlow (NetFlow/sFlow) sensors?
- http://www.paessler.com/knowledgebase/en/topic/483

Knowledge Base: How do the channel definitions for custom Packet Sniffing or xFlow (NetFlow/sFlow) sensors work?
- http://www.paessler.com/knowledgebase/en/topic/473

Knowledge Base: Does my Cisco device (Router/Switch) support NetFlow Export?
- http://www.paessler.com/knowledgebase/en/topic/5333

Knowledge Base: Do you have any configuration tips for Cisco routers and PRTG?
- http://www.paessler.com/knowledgebase/en/topic/563

Knowledge Base: Is it possible to monitor Cisco ASA Firewalls using Netflow 9 and PRTG?
- http://www.paessler.com/knowledgebase/en/topic/633

Knowledge Base: How to monitor Cisco ASA Firewalls using NetFlow 9 and PRTG?
- http://www.paessler.com/knowledgebase/en/topic/1423

Tools: NetFlow Generator and NetFlow Tester
- http://www.paessler.com/tools/

© 2011 Paessler AG

10.5 Bandwidth Monitoring Comparison

The following table shows the differences between PRTG's four methods available for bandwidth monitoring:

© 2011 Paessler AG

	WMI	SNMP	Packet Sniffer	xFlow (Netflow, sFlow, jFlow)
Setup	Medium	Easy	Easy to Complex (depending on filter rules used)	Can be complex (e.g. the switch must be configured)
Traffic can be filtered	No	No	Yes	Yes
Differentiate bandwidth usage by protocol or IPs	No	No	Yes	Yes
PRTG can show Toplists (Top Talker, Top Connections, Top Protocols etc.)	No	No	Yes	Yes
Filter bandwidth usage by IP	No	No	Yes	Yes
Filter bandwidth usage by MAC address	No	No	Yes	No
Filter bandwidth usage by physical network port	Yes	Yes	No	No
Monitor network parameters other than bandwidth usage	Yes	Yes	No	No
CPU load on the machine running PRTG	Low	Low	Higher, depends on the amount of traffic	Higher, depends on the amount of traffic
Excess bandwidth usage of monitoring	Small	Small	None (except when monitoring switch ports are used)	Depends on the traffic

More

Knowledge Base: Should I use SNMP, xFlow (NetFlow/sFlow) or Packet Sniffing for my monitoring?

- http://www.paessler.com/knowledgebase/en/topic/923

Knowledge Base: How do I discern excessive bandwidth usage with PRTG?

- http://www.paessler.com/knowledgebase/en/topic/2923

© 2011 Paessler AG

10.6 Monitoring Quality of Service

PRTG can monitor the Quality of Service in a network with its own QoS sensor as well as Cisco IP Service Level Agreement (SLA). Slight variations of network parameters like jitter, packet loss, or packet delay variation (PDV) usually have only little effect on TCP based services (e.g. HTTP, SMTP, etc.). But for UDP based services like Voice over IP (VoIP) and video streaming a steady stream of data packets is crucial. The sound quality of a VoIP call drops dramatically when UDP packets are not received in a timely fashion, or if packets are lost or out-of-order. As a rule of thumb for good quality of service (in a VoIP perspective) you would want low measurements for jitter (less than 20 to 50 ms) and PDV (less than 100 ms) and preferably *zero* measurements for packet loss, duplicated packets, or packets in wrong order.

For Quality of Service measurements, two sensors are available:

- **QoS (Quality of Service) Sensor** 481
  Monitors VoIP relevant network parameters by testing network connection quality between two probes.

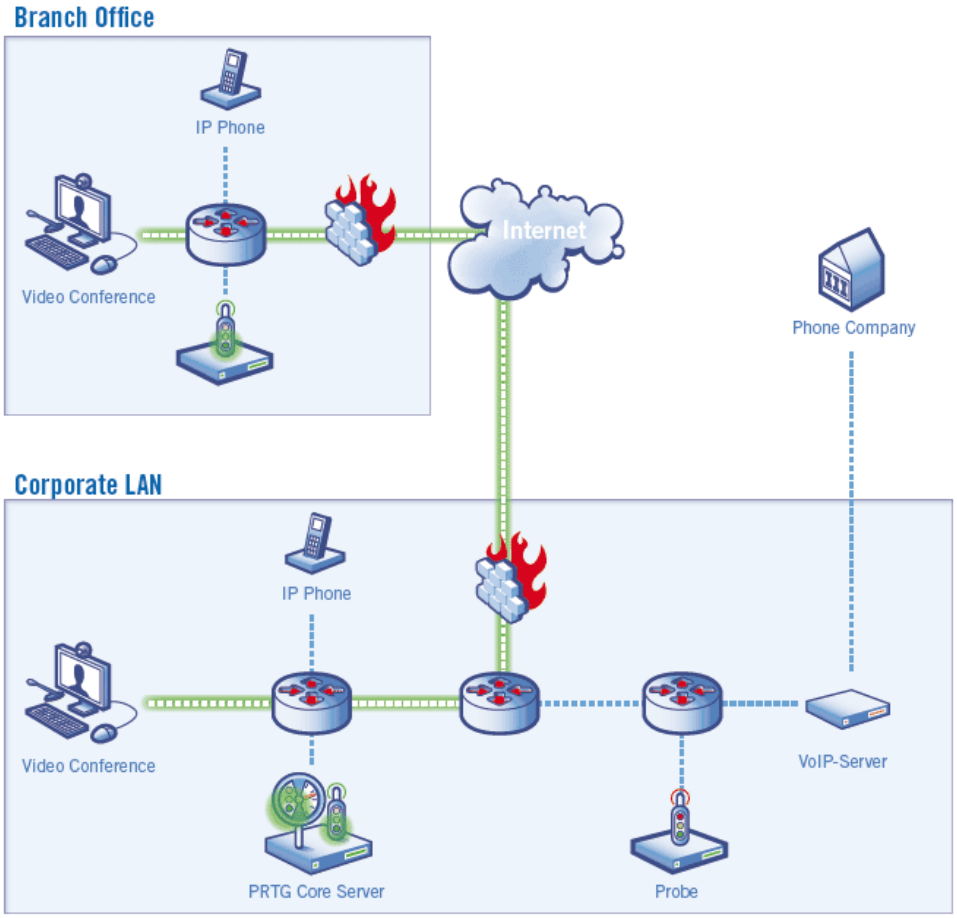
- **Cisco IP SLA Sensor** 226
  Monitors VoIP relevant network parameters through IP SLA results from Cisco devices (via SNMP).

QoS (Quality of Service) Sensor

The QoS Sensor is used to monitor the quality of a network connection by measuring the following parameters:

- Jitter in ms according to RFC 3550
- Packet delay variation (PDV) in ms according to RFC 3393
- Lost packets in %
- Out-of-order packets in %
- Duplicated packets in %

The measurements are taken by sending UDP packets between two probes. This means that you can test any network connection in your network by simply placing a remote probe 986 on (or near) each 'end' of the connection and measuring the connection quality between them. This is the perfect tool to find network issues that can affect VoIP sound quality or video streaming 'hiccups'.



Monitoring Quality of Service with PRTG

As mentioned before, measurement are taken between two probes. So the first step is to place two PCs running a remote probe on (or near) both ends of the connection that you want to monitor. As an alternative, the local probe on the PC running the PRTG core can also be used as one end. If any firewalls, packet filters or Network Address Translation (NAT) systems are en route, you must configure them as necessary so that the UDP packets can reach the target probe.

In PRTG, create a new QoS sensor on a **Probe Device**. Please find details about settings in the QoS (Quality of Service) Sensor 481 section. With the settings for number and for size of the packets you can configure the test data stream. 1,000 packets of 172 bytes each is a good start, but if your applications use larger packets you may want to enter other values here. Try to configure the test streams with parameters similar to that of the UDP services you are using across this connection.

Cisco IP SLA Sensor

Wikipedia describes IP SLA as *a feature included in the Cisco IOS Software that can allow administrators the ability to Analyze IP Service Levels for IP applications and services. IP SLA uses active traffic-monitoring technology to monitor continuous traffic on the network. This is a reliable method in measuring over head network performance.* IP-SLA is mostly used to monitor the sound quality of VoIP traffic.

© 2011 Paessler AG

If you haven't done so already, please add a device in PRTG for the Cisco device that you want to monitor. Then create a new **Cisco IP SLA** sensor on this device. Please find details about settings in the Cisco IP SLA Sensor 226 section.

This feature is only available in the more expensive Cisco devices. If you don't have IP SLA capable routers/switches you can still get similar information with PRTG's QoS sensor (see above 947) which does not require any special hardware—just two PCs running Windows. If you do own hardware which supports IP SLA then PRTG brings you probably the least-cost monitoring solution for IP SLA. Most vendors charge extra for IP SLA support (a thousand bucks and more). Following Paessler's long term policy we simply include this as one of our sensor types. With PRTG you can even use the Freeware Edition to monitor IP SLA!

PRTG monitors the following parameters: Calculated Planning Impairment Factor (ICPIF), Mean Opinion Score (MOS), Average Jitter, Packets Lost, Packets Out Of Sequence, Packets Late, Average Round Trip Time (RTT), DNS RTT, TCP RTT, Transaction RTT. Especially two of these parameters are interesting for VoIP: Mean Opinion Score (MOS) and Calculated Planning Impairment Factor (ICPIF).

Voice over IP

For Mean Opinion Score (MOS) measurements, Cisco conducted a panel test where a wide range of listeners judged the quality of voice samples sent using particular codecs, on a scale of 1 (poor quality) to 5 (excellent quality). The Cisco device calculated the corresponding value for the current network connection based on the network parameter measurements like jitter and packet loss. The values and their meanings are:

MOS	Quality	Expected Quality Impairment
5	Excellent	Imperceptible
4	Good	Perceptible, but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

The second interesting parameter ICPIF *is the sum of measured impairment factors minus a user-defined access Advantage Factor that is intended to represent the user's expectations, based on how the call was placed (for example, a mobile call versus a land-line call)* (quoted from Cisco's website).

Upper Limit for ICPIF	VoIP Call Communication Quality
5	Very good
10	Good
20	Adequate
30	Limiting case
45	Exceptional limiting case
55	Customers likely to react strongly (complaints, change of network operator)

More

Paessler Knowledge Base: Where can I find more information about Cisco IP SLAs, VoIP, and QoS?

- http://www.paessler.com/knowledgebase/en/topic/11093

© 2011 Paessler AG

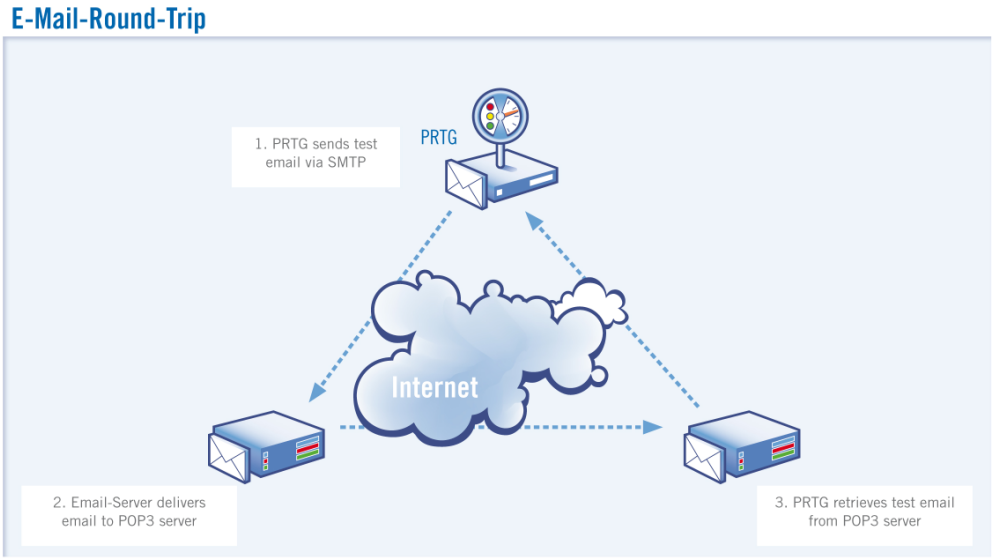
10.7 Monitoring Email Round Trip

Email Round Trip sensors ensure the end-to-end delivery of emails and make it possible to monitor availability and performance of a complete email delivery process. There are two sensor types for this task:

- SMTP&POP3 Round Trip Sensor 534
- SMTP&IMAP Round Trip Sensor 527

Both initially deliver an email to a mail server using SMTP. Afterwards the receiving mailbox is scanned using Post Office Protocol version 3 (POP3) or Internet Message Access Protocol (IMAP) until the email arrives. The test email contains a unique code in the topic which is used to identify the email, such as *PRTG8 Roundtrip Mail: {6D136420-5A3E-46CF-871A-1DAF0C4F3D5D}*.

When PRTG successfully received an email in this email round trip cycle, it marks the respective message for deletion on the mail server. Usually, a mail server will then delete this email. For best performance, we recommend using a dedicated email accounts for email round trip sensors.


E-Mail-Round-Trip
1. PRTG sends test email via SMTP
PRTG
Internet
2. Email-Server delivers email to POP3 server
3. PRTG retrieves test email from POP3 server

Monitoring an Email Round Trip

In the scenario shown above, there are three steps in the round trip:

- **Step 1**
  PRTG delivers an email via the SMTP protocol to a mail server (just like an email client).

- **Step 2**
  The SMTP server delivers the email to a POP3/IMAP server (which can be located at a remote site, in your local LAN or on the same server as well).

- **Step 3**
  Every few seconds PRTG connects to the POP3/IMAP server until the test email arrives.

Recommended Configuration

Here is a simple concept to check delivery of email out of and into your organization:

1. Create a dedicated email account for this test in your mail system.

2. Set up an external email account (hosted mail server, free mail service, etc.) and configure it to send all emails back to this dedicated email account in your organization (which you created in *Step 1*).

3. Set up PRTG's round trip sensor to send an email to the external email account (which you created in *Step 2*) using your LAN's mail server and then check for the email account on your mail system (which you created in *Step 1*) for arrival of the email.

With this technique you are testing multiple aspects of your email server setup. As long as the sensor shows a green light, this means:

- Your email server accepts emails via SMTP.
- Emails are being sent to the outside world (internet connection works, MX lookups work etc.).
- Emails from external mail server can be delivered into your mail system (this includes aspects like the fact that the MX records for your domain are correct, your mail server can be reached from the outside world, your email filtering is working etc.).
- Emails can be retrieved using POP3 (or IMAP).

Conclusion

These two sensor types are a great tool to ensure delivery of email from and to your mail servers. Compared to the standard SMTP, POP3 and IMAP sensors - which only check the availability of these services - the two roundtrip sensor types actually monitor the complete transaction from accepting the mail on the first email server to delivery of the mail on the final POP3/IMAP server.

© 2011 Paessler AG

Part XI

System Administration Programs

11 System Administration Programs

Using the two administration programs **PRTG Server Administrator** and **PRTG Probe Administrator** you can edit administrative settings that affect your PRTG installation, the local probe running with it, or a remote probe installation. All settings will require a restart of the Windows services for changes to take effect. Please see these following sections.

System Administration Programs—Topics

- PRTG Server Administrator 955
- PRTG Probe Administrator 969

Related Topics

- Setup 857

© 2011 Paessler AG

11.1 PRTG Server Administrator

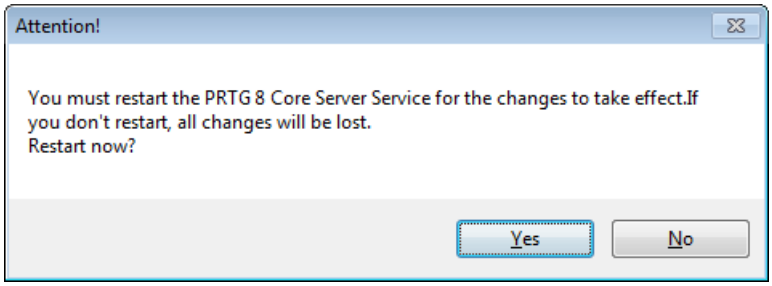
In the PRTG Server Administrator program you can define different system-oriented settings that affect your PRTG installation, as well as restart services and view log information. *Note:* To get familiar with the different components of PRTG, we recommend reading the **Architecture** 75 section.

Note: All settings made here are only valid for the local installation running on the computer you're opening the program on. In order to change settings for another installation, for example, another cluster node installation, please log in to this computer and open the program there.

From the **PRTG Network Monitor** group in Windows start menu, please select **PRTG Server Administrator** to open the application. You can choose from these options in different tabs:

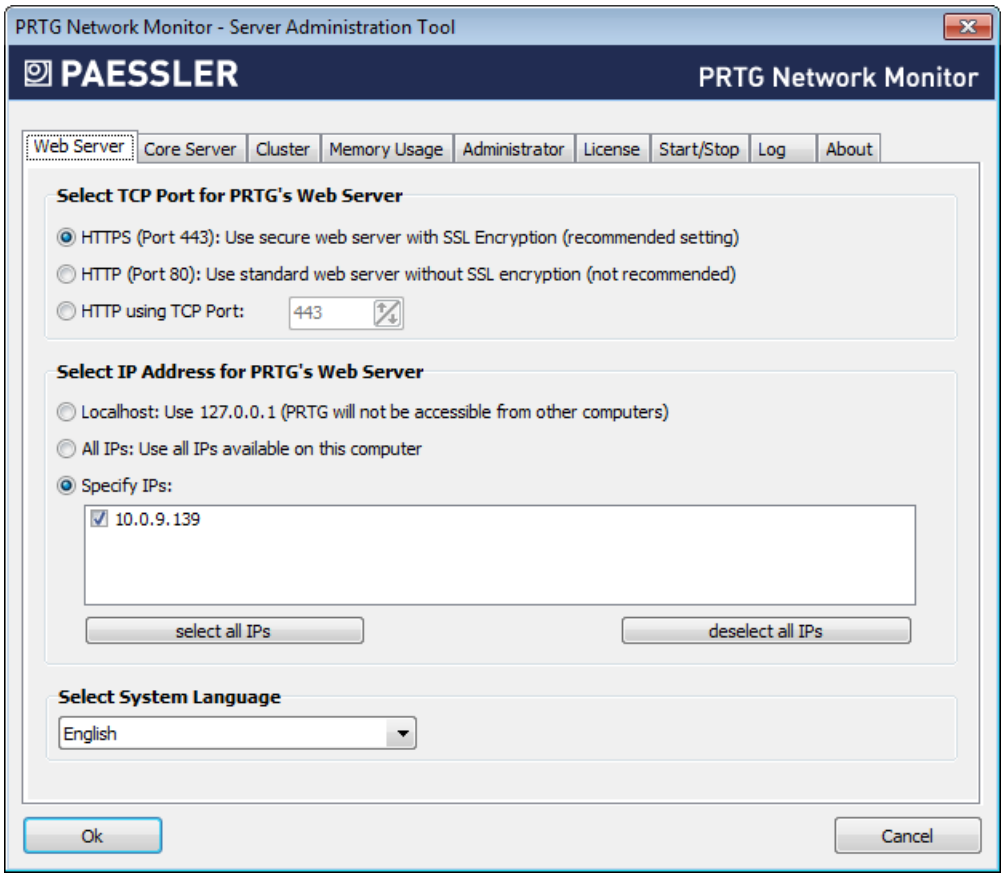
- Web Server 955
- Core Server 957
- Cluster 959
- Memory Usage 960
- Administrator 963
- License 964
- Start/Stop 965
- Logs 966
- About 968

When closing the program using the **Ok** button, you are asked to restart the core server Windows service in order to save the settings. Please confirm by clicking the **Yes** button. Otherwise the changes are ignored.


Attention!
You must restart the PRTG 8 Core Server Service for the changes to take effect.If you don't restart, all changes will be lost.
Restart now?
Yes
No

Web Server

Edit IPs, ports, access methods and language for the Ajax 92 and HTML GUI 927 web interfaces.



Web Server—Select TCP Port for PRTG's Web Server

PRTG is running a web server in order to provide the web and Windows interface. Please specify on which port this web server will run.

HTTPS (Port 443)

- This is the recommended setting.
- Use a secure HTTPS connection that is encrypted via SSL on port 443.
- SSL-secured connections can be established on port 443 only.
- *Note:* Although the connection is secure, you will see a certificate warning in your browser when logging in to the PRTG web interface, because the default certificate is unknown to your browser. You can install another SSL certificate for PRTG later. Please see the More 52 section below.
- *Note:* If port 80 is free, PRTG will reserve it as well. When users try to connect on port 80 via HTTP, they will then be redirected to port 443 via HTTPS. You can change this behavior later. Please see the More 52 section below.

HTTP (Port 80)

- This setting is not recommended for WAN connections.
- Use a standard web server without SSL encryption on port 80.
- *Note:* If used on the Internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend using this option in a LAN only.

© 2011 Paessler AG

HTTP using TCP Port

- This setting is not recommended for WAN connections.
- Use a standard web server without SSL encryption on a custom port.
- This option is intended for systems with an existing web server.
- Enter the desired TCP port you want the PRTG web server to run on.
- *Note:* If used on the Internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend using this option in a LAN only.

Web Server—Select IP Address for PRTG's Web Server

PRTG is running a web server in order to provide access via the web and Windows interface. Please specify which IP address this web server will run on. *Note:* Later, you can log into PRTG by simply pointing your browser to the specified IP address.

Localhost

- Use *127.0.0.1* only.
- PRTG's web and Windows interface will only be accessible from the computer PRTG is installed on.
- *Note:* Either the selected port or at least one port in the range from **8080** to **8089** has to be available on *127.0.0.1*.

All IPs

- Use all IP addresses available on this computer and enable access to the web server for all of these addresses.
- *Note:* The TCP port selected above must be free on every available IP address.

Specify IPs

- Select specific IP addresses on which the PRTG Web server will run on.
- A list specific to your system is shown.
- Add a check mark in front of every IP address you want the PRTG web server to be available at.
- *Note:* Either the selected port or at least one port in the range from **8080** to **8089** has to be available on the specified IP address.

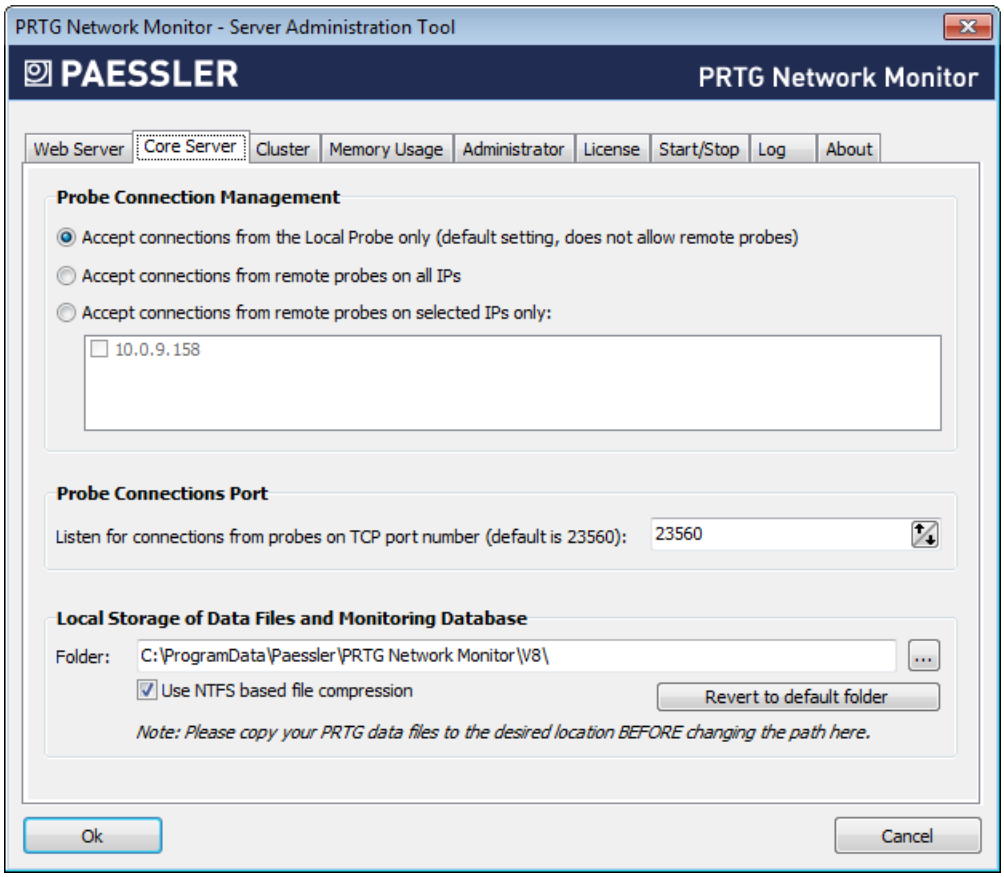
Note: Regardless of the selected setting above, one port in the range from **8080** to **8180** has to be available on the specified IP address so PRTG can create reports. The report engine will try to connect to the core server on one of these ports.

Select System Language

- Choose the language for this program from the drop down menu. Default is **English**. Depending on your installation, you may be able to choose other languages here.
- This setting will influence the language of this program, as well as the Ajax 92 and the HTML GUI 927 web interfaces.

Core Server

Define settings for the core server.


PRTG Network Monitor - Server Administration Tool
PAESSLER
PRTG Network Monitor
Web Server
Core Server
Cluster
Memory Usage
Administrator
License
Start/Stop
Log
About
Probe Connection Management
Accept connections from the Local Probe only (default setting, does not allow remote probes)
Accept connections from remote probes on all IPs
Accept connections from remote probes on selected IPs only:
10.0.9.158
Probe Connections Port
Listen for connections from probes on TCP port number (default is 23560):
23560
Local Storage of Data Files and Monitoring Database
Folder:
C:\ProgramData\Paessler\PRTG Network Monitor\V8\
Use NTFS based file compression
Revert to default folder
Note: Please copy your PRTG data files to the desired location BEFORE changing the path here.
Ok
Cancel

Core Server—Probe Connection Management

In this section you can define how PRTG handles incoming connections from probes. Choose between several options.

Accept connections from the Local Probe only

- This is the default setting.
- Only local probe connections will be accepted by the PRTG core server.
- You cannot use remote probes 986 with this setting enabled.

Accept connections from remote probes on all IPs

- Incoming connections from remote probes will always be accepted, no matter on which IP address of the core server they come in.

Accept connections from remote probes on selected IPs only

- Incoming connections from remote probes 990 will only be accepted on the selected IP address(es) of the core server.
- In the list, select the IP addresses by adding a check mark in front the IPs.

© 2011 Paessler AG

Core Server—Probe Connections Port

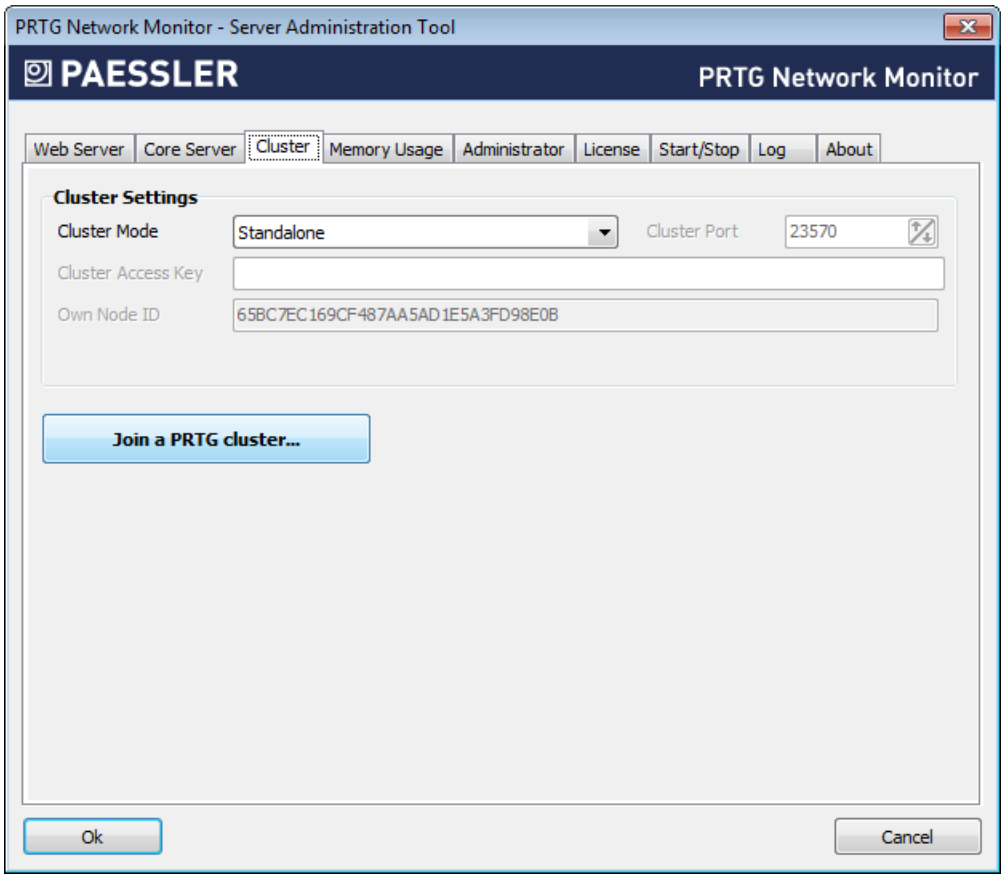
In this section you can define on which TCP port number PRTG listens to for incoming probe connections. Enter a port number. We recommend using the default value.

Core Server—Local Storage of Data Files and Monitoring Database

- Define the data folder to which PRTG will store configuration and monitoring data. Define a path or click on the **Revert to default folder** to reset to default. *Note:* Before changing the path, make sure you stop both services and copy all data to the new location.
- When enabling the **Use NTFS based file compression** option, you will save disk space, but you will experience a higher CPU load on the core system.

Cluster

In the **Cluster** tab you can manually change how the current core installation will behave in a cluster. Before changing settings here, please read Install a PRTG Cluster 53 section.



Cluster Mode

Depending on the current installation, you can choose between different cluster modes.

- **Standalone**: Do not integrate the current core installation in a PRTG cluster, but run a standalone installation only.
- **Cluster Node: Master Node**: Make this core installation the master node of a cluster. In every cluster there may only exist one master node.
- **Cluster Node: Failover Node**: Make this core installation a failover node in a cluster. There may be several failover nodes in one cluster. This option is only available on installations that are already configured as a failover node. In order to convert a standalone or master node installation into a failover node, you have to join the cluster. Please see **More** 968 section below for detailed instructions on how to join an existing cluster.

Cluster Access Key

- This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.

Own Node ID

- This field is shown for information purposes only. It shows the automatically generated node ID which identifies the current core installation in the cluster.

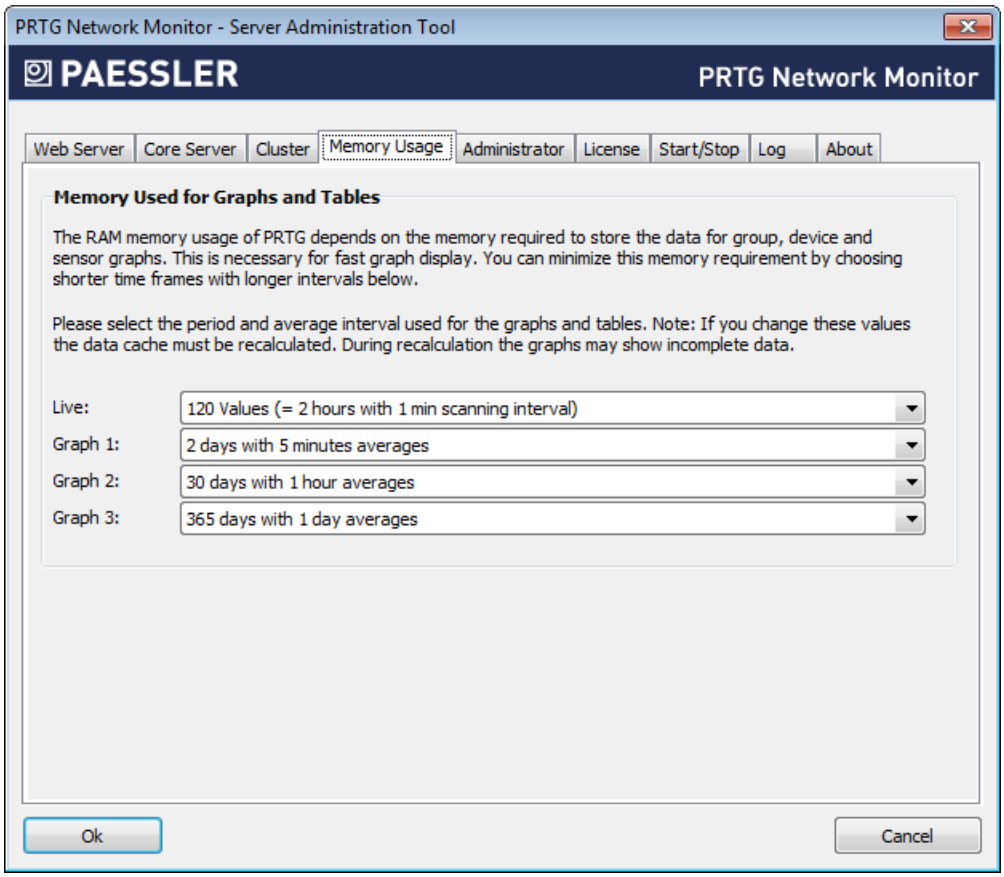
Join a PRTG cluster...

- Click the **Join a PRTG cluster...** button to start an assistant that helps you join this installation of PRTG as a failover node into an existing cluster. Please see **More** 968 section below for detailed instructions on this.

Memory Usage

PRTG shows several graphs in the object's detail pages 104 in the web interface. These are saved in RAM memory for fast display without causing extra CPU load or disk usage. The longer the time frames and the shorter the intervals are, the more memory will be used. You can adapt the details for all four graphs. This setting will also affect the description of the object's tabs in the web interface.

© 2011 Paessler AG


PRTG Network Monitor - Server Administration Tool
PAESSLER
PRTG Network Monitor
Web Server
Core Server
Cluster
Memory Usage
Administrator
License
Start/Stop
Log
About
Memory Used for Graphs and Tables
The RAM memory usage of PRTG depends on the memory required to store the data for group, device and sensor graphs. This is necessary for fast graph display. You can minimize this memory requirement by choosing shorter time frames with longer intervals below.
Please select the period and average interval used for the graphs and tables. Note: If you change these values the data cache must be recalculated. During recalculation the graphs may show incomplete data.
Live:
120 Values (= 2 hours with 1 min scanning interval)
Graph 1:
2 days with 5 minutes averages
Graph 2:
30 days with 1 hour averages
Graph 3:
365 days with 1 day averages
Ok
Cancel

Live

For the live graph, no fixed time span is given, but you can define how many values will be displayed. The actual time span covered by the live graph depends on the scanning interval set for the object you're viewing the graph of. As example, the time span for the default interval of one minute is given. Other intervals will result in different time spans. Choose between:

- **60 Values**: This corresponds to a live graph covering a time span of one hour if a 1 minute scanning interval is set.
- **120 Values**: This corresponds to a live graph covering a time span of two hours if a 1 minute scanning interval is set.
- **240 Values**: This corresponds to a live graph covering a time span of four hours if a 1 minute scanning interval is set.
- **480 Values**: This corresponds to a live graph covering a time span of eight hours if a 1 minute scanning interval is set.
- **960 Values**: This corresponds to a live graph covering a time span of 16 hours if a 1 minute scanning interval is set.

Graph 1

By default, this is the **2 days** graph in the web interface. You can change it to more or less detail by choosing a time span covered and a monitoring interval average associated with it. Choose between:

- **1 day with 1 minute averages**

- **1 day with 5 minutes averages**
- **1 day with 15 minutes averages**
- **2 days with 1 minute averages**
- **2 days with 5 minutes averages**
- **2 days with 15 minutes averages**
- **4 days with 1 hour averages**

Graph 2

By default, this is the **30 days** graph in the web interface. You can change it to more or less detail by choosing a time span covered and a monitoring interval average associated with it. Choose between:

- **10 days with 1 hour averages**
- **20 days with 1 hour averages**
- **30 days with 1 hour averages**
- **30 days with 6 hour averages**
- **40 days with 1 hour averages**
- **40 days with 6 hour averages**
- **60 days with 1 hour averages**
- **60 days with 6 hour averages**

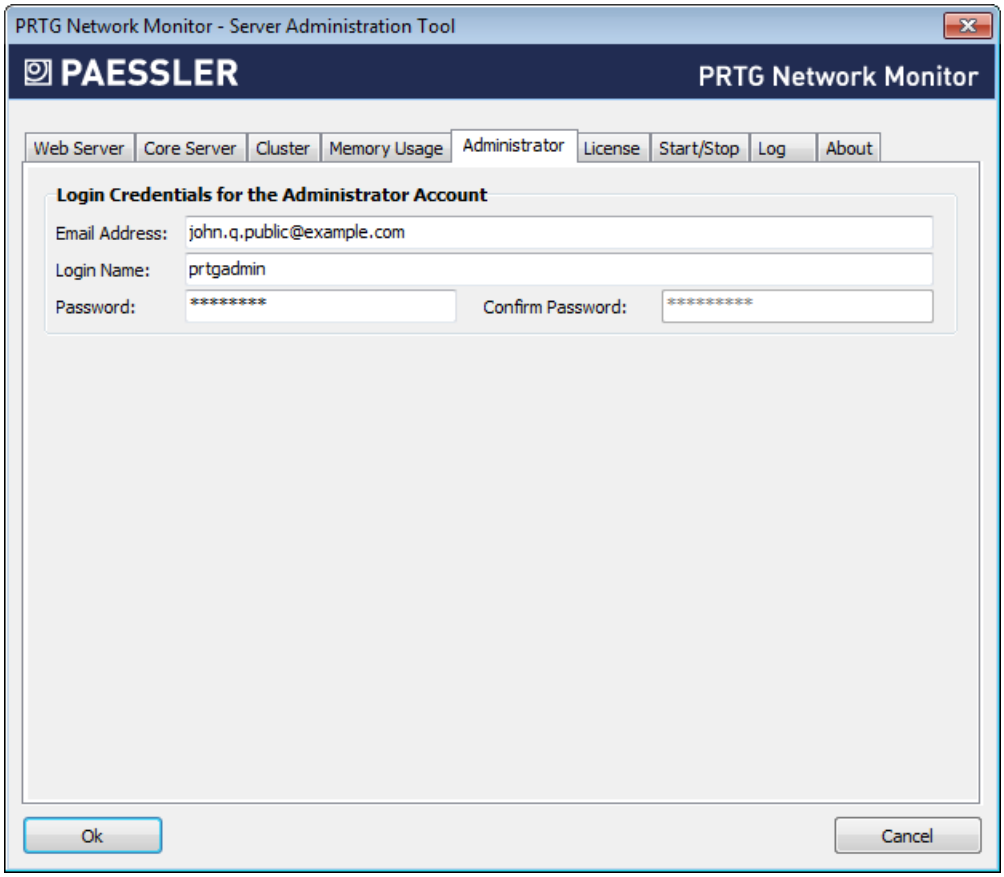
Graph 3

By default, this is the **365 days** graph in the web interface. You can change it to more or less detail by choosing a time span covered and a monitoring interval average associated with it. Choose between:

- **100 days with 1 day averages**
- **200 days with 1 day averages**
- **365 days with 1 day averages**
- **400 days with 1 day averages**
- **750 days with 1 day averages**

© 2011 Paessler AG

Administrator



Enter the administrator's contact email address and define login credentials for PRTG.

Email Address

- Enter a valid administrator's email address.
- By default, PRTG will send notifications and important messages to this address.

Login Name

- Enter a name for the PRTG administrator login; this is your default login.
- It is used when logging in to the PRTG Web- or Windows interface.
- If you do not change this setting, the default login name **prtgadmin** is used.

Password

- Enter a password for the PRTG administrator login; this is your default login.
- It is used when logging in to the PRTG Web- or Windows interface.
- If you do not change this setting, the default password **prtgadmin** is used.

Confirm Password

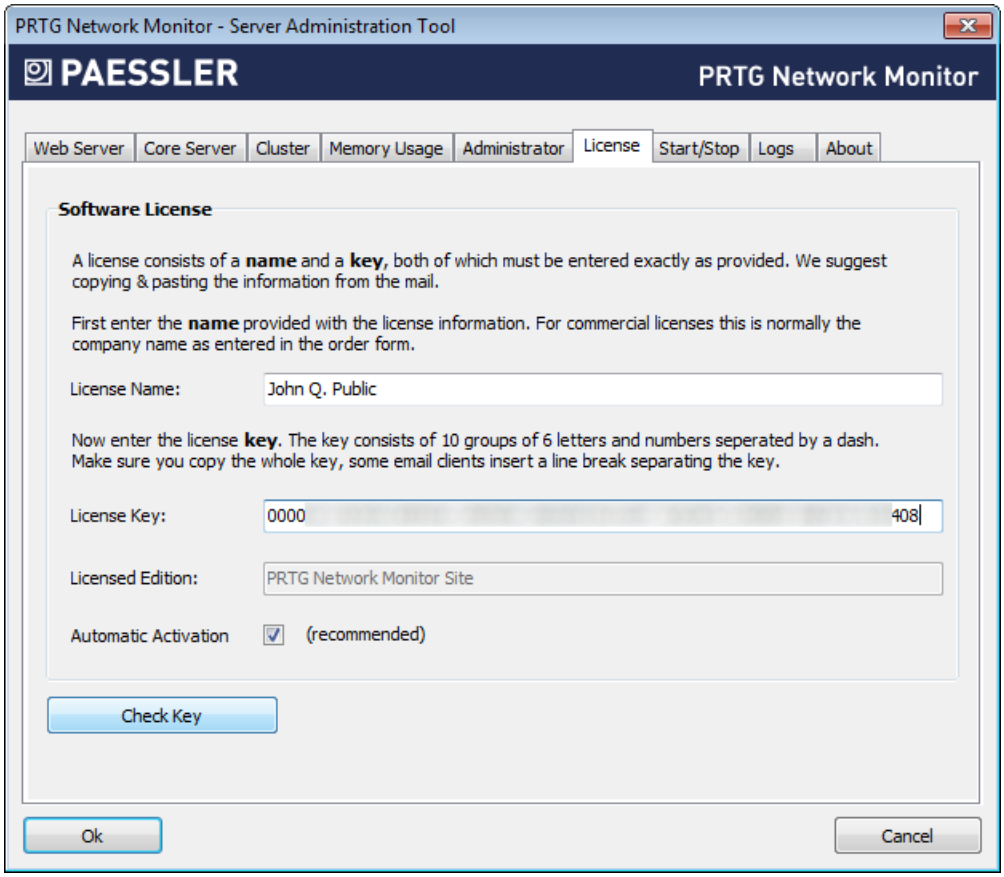
- Re-enter the password for the PRTG administrator login.

© 2011 Paessler AG

- If you do not change this setting, the default password **prtgadmin** is used.

License

To use a PRTG license with this installation of PRTG, please enter the license information you have received from Paessler via email. To avoid typing errors, please copy and paste the name and the key from the email.


PRTG Network Monitor - Server Administration Tool
PAESSLER
PRTG Network Monitor
Web Server
Core Server
Cluster
Memory Usage
Administrator
License
Start/Stop
Logs
About
Software License
A license consists of a name and a key, both of which must be entered exactly as provided. We suggest copying & pasting the information from the mail.
First enter the name provided with the license information. For commercial licenses this is normally the company name as entered in the order form.
License Name:
John Q. Public
Now enter the license key. The key consists of 10 groups of 6 letters and numbers seperated by a dash. Make sure you copy the whole key, some email clients insert a line break separating the key.
License Key:
0000
408
Licensed Edition:
PRTG Network Monitor Site
Automatic Activation
(recommended)
Check Key
Ok
Cancel

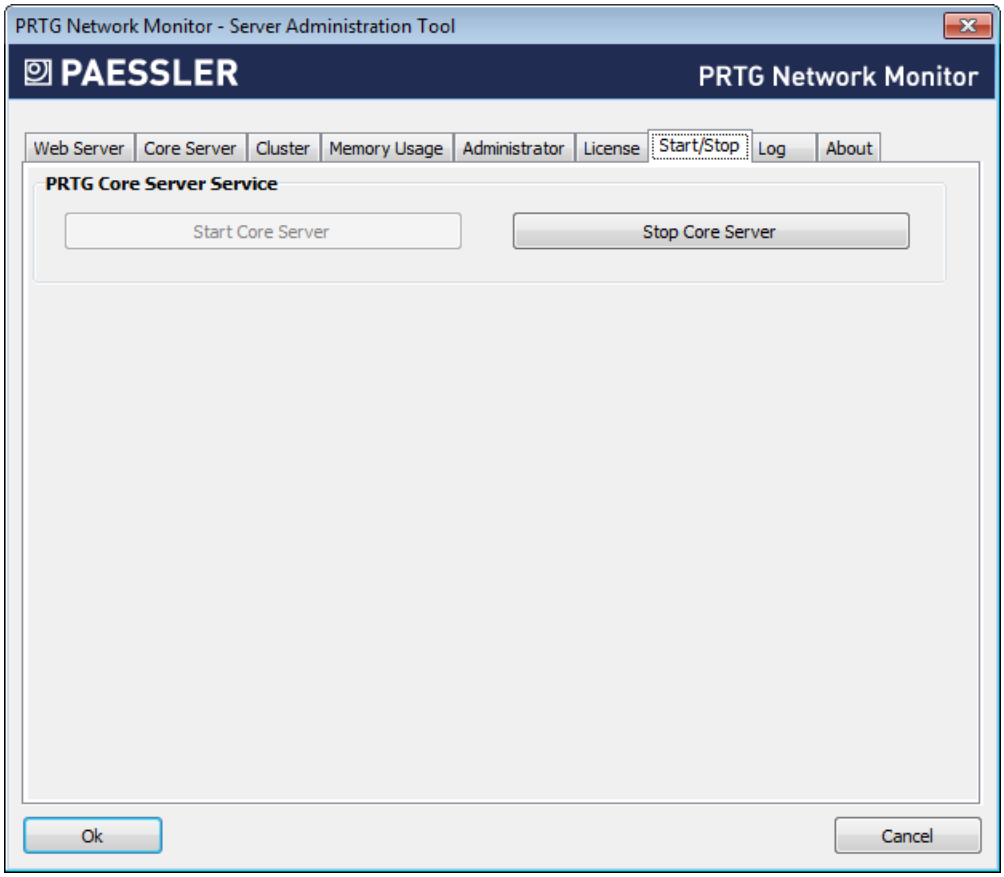
PRTG Server Administrator License Tab

To make sure your key has been entered correctly please click on the **Check Key** button. A popup box will either show success or denial of your license information. In the **Licensed Edition** field you will see an accepted licence key. Please remember to activate your license in the web interface. For more details, please see Activate the Product 57 section.

Note: You have to use the right edition for your license key. For example, the installer for trial and Freeware edition does not accept any commercial keys. For more information, please see Enter a License Key 55 section.

© 2011 Paessler AG

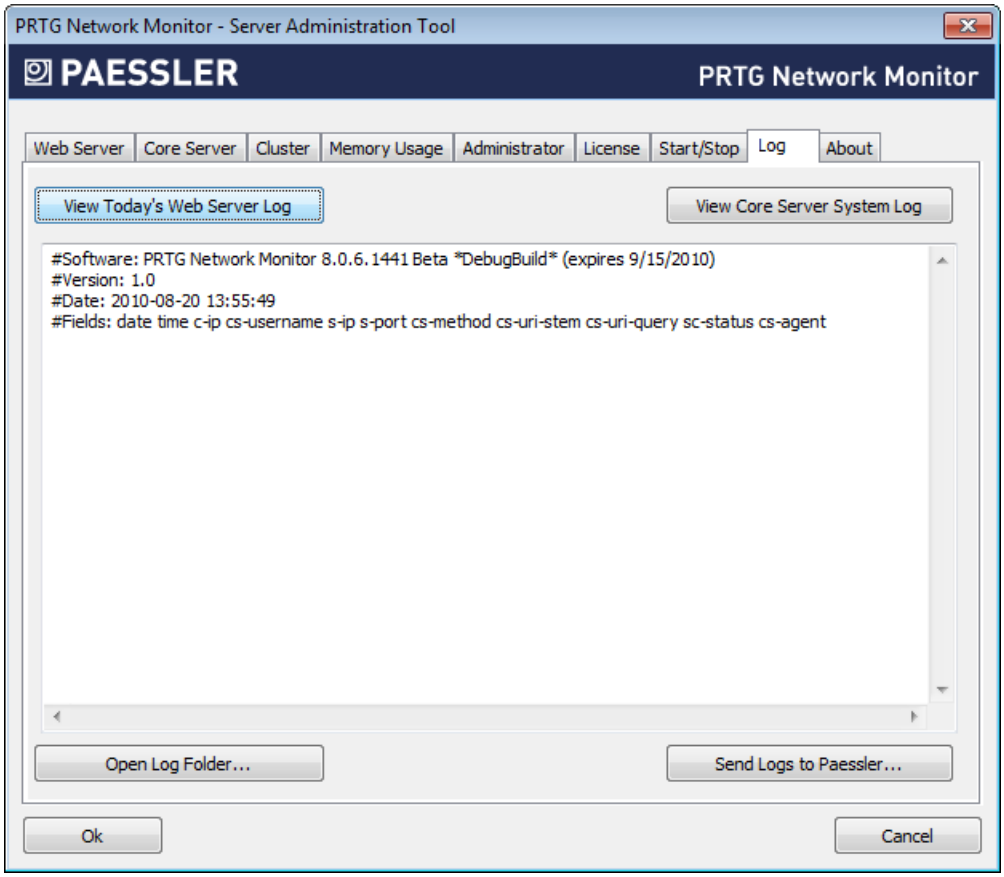
Start/Stop



You can stop and start the core server Windows service manually. Click the **Stop Core Server** button to stop the service, and **Start Core Server** to start it again. Both actions usually take from a few seconds up to several minutes to complete.

Note: If you want to schedule an automatic restart of Windows services for both core server and probe service, please do so using the **PRTG Probe Administrator**. For more details see PRTG Probe Administrator 971 (Start/Stop) section.

Logs



You can view several logs of your PRTG installation. The following buttons are available:

- **View Today's Webserver Log**
  Directly view the content of the web server log for the current date.

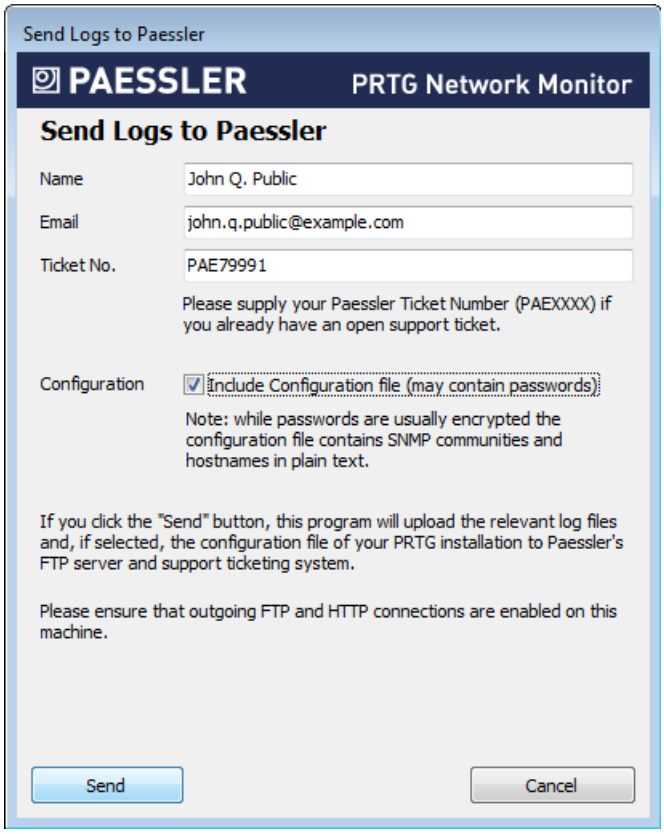
- **View Core Server System Log**
  Directly view the content of the core server system log. Depending on the number of entries, it may take a few seconds until the logs are shown.

- **Open Log Folder...**
  Open the log file directory on your hard disk drive to access older web log files, etc.

- **Send Logs to Paessler...**
  Open an assistant to send log files to the Paessler support team. Please see below.

© 2011 Paessler AG

Logs—Send Logs to Paessler


Send Logs to Paessler
PAESSLER PRTG Network Monitor
Send Logs to Paessler
Name
John Q. Public
Email
john.q.public@example.com
Ticket No.
PAE79991
Please supply your Paessler Ticket Number (PAEXXXX) if you already have an open support ticket.
Configuration
Include Configuration file (may contain passwords)
Note: while passwords are usually encrypted the configuration file contains SNMP communities and hostnames in plain text.
If you click the "Send" button, this program will upload the relevant log files and, if selected, the configuration file of your PRTG installation to Paessler's FTP server and support ticketing system.
Please ensure that outgoing FTP and HTTP connections are enabled on this machine.
Send
Cancel

When opening a support ticket, Paessler support may ask you to send log files for further analysis. Using the **Send Logs to Paessler...** button, PRTG will automatically collect, compress and send your log files.

Name

- Please enter your name.

Email

- Please enter your valid email address.

Ticket No.

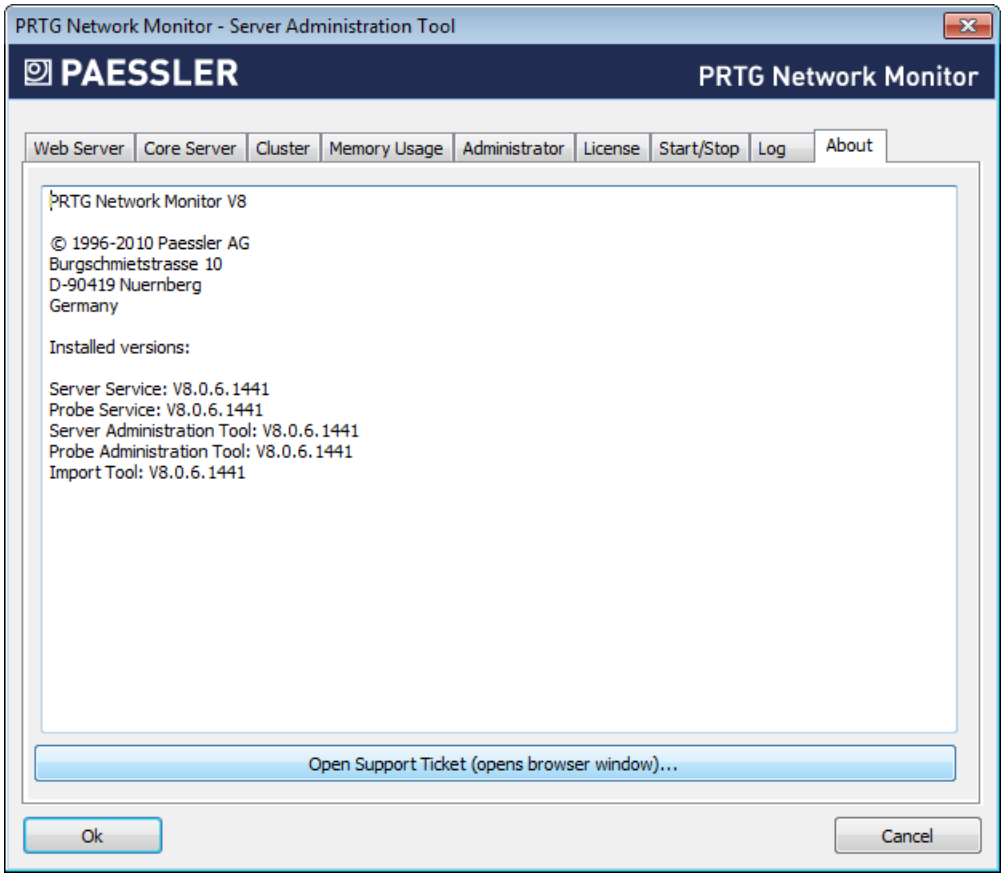
- This field is optional.
- If you have already opened a ticket at Paessler support, please provide the ticket number you received. Your files will then be associated with your ticket automatically.
- Please enter the ticket number starting with **PAE** followed by four or more digits.
- If you do not have a ticket number, please leave the field empty. *Note:* You should usually contact the support team *before* sending any files.

Configuration

- Define if your configuration file will be included in the data. Passwords are usually encrypted, but there may be some passwords stored as plain text.

Click on the **Send** button to start data upload. Please make sure FTP and HTTP connections are allowed on this machine.

About



Displays version information for installed PRTG programs. Click on the **Open Support Ticket** button to ask the Paessler support team for help. This will open a new web browser window.

More

Knowledge Base: 10 Steps to Set Up a Cluster—Scenario 3: You've Set Up Two PRTG 8 Installations Already

- http://www.paessler.com/knowledgebase/en/topic/6923

© 2011 Paessler AG

11.2 PRTG Probe Administrator

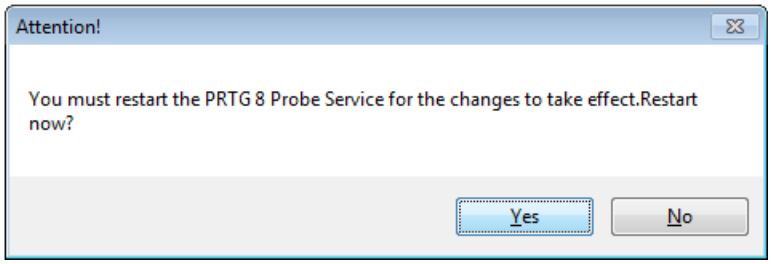
In the PRTG Probe Administrator program, you can define different system-oriented settings that affect your PRTG installation, as well as restart services and define the data storage location. *Note:* To get familiar with the different components of PRTG, we recommend reading the **Architecture** 75 section.

Note: All settings made here are only valid for the local installation running on the computer you're opening the program on. In order to change settings for another installation, for example, another remote probe installation, please log in to this computer and open the program there.

From the **PRTG Network Monitor** group in Windows start menu, please select **PRTG Probe Administrator** to open the application. You can choose from these options in different tabs:

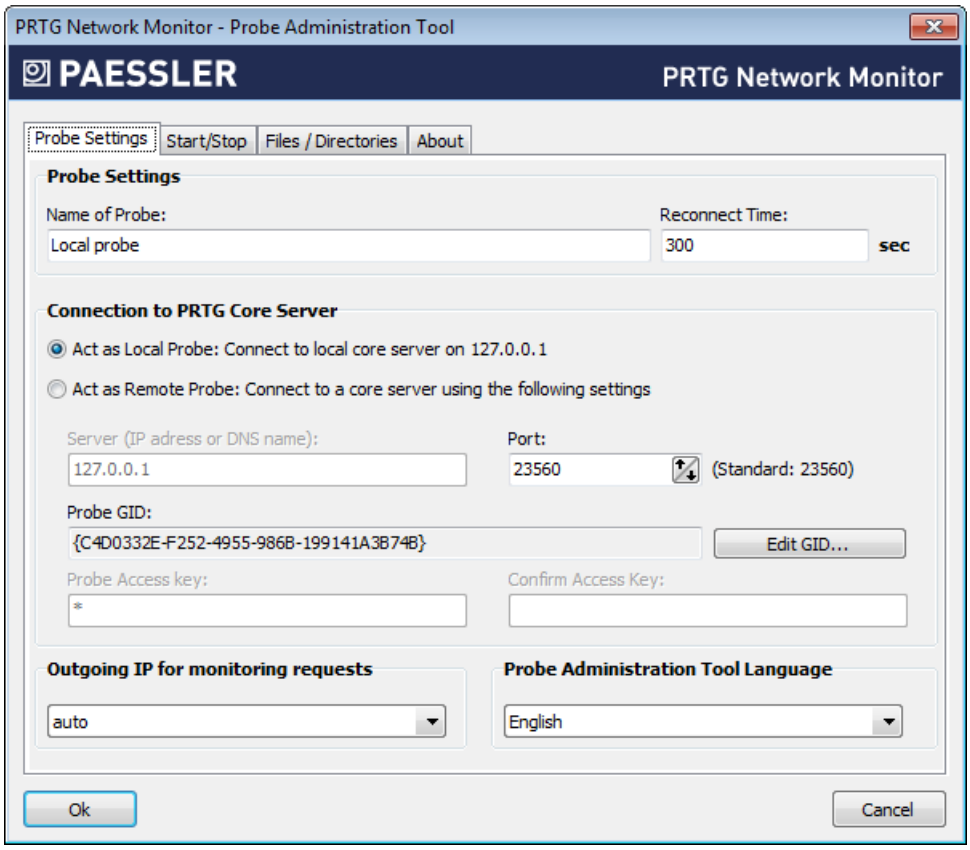
- Probe Settings 969
- Start/Stop 971
- Logs/Directory 973
- About 976

When closing the program using the **Ok** button, you are asked to restart the probe Windows service in order to save the settings. Please confirm by clicking the **Yes** button.



Probe Settings

Define general settings regarding the probe and probe connections.



Probe Settings—Probe Settings

Name of Probe

- Enter a name for the probe. It will appear in the device tree in the web interface.

Reconnect Time

- Define the time that will be waited until the probe tries to reconnect to the core server in case the connection fails.

Probe Settings—Connection to PRTG Core Server

These settings will affect how the probe will connect to the core server. A probe is either a local probe or a remote probe.

Act as Local Probe

- This probe will act as the local probe of the PRTG core installation.
- It will connect to the core via *127.0.0.1*.
- No access key is needed for local probe connections.

Act as Remote Probe

© 2011 Paessler AG

- This probe will act as remote probe.
- We recommend using this setting only for remote probe installations 59. On the system running the PRTG core server, you should not change a local probe to a remote probe!
- Enter the Server IP address or DNS name and the port for the connection to the core server.
- The **Probe GID** is a unique identifier for the probe and should not be changed. Except when substituting an existing probe, you must change it to the old probe's GID. To do so, click on the **Edit GID...** button and confirm the warning with **Yes**. You can then change the value.
- The **Probe Access key** must match one of the access keys configured in your PRTG core server installation. If it doesn't, the remote probe will not be able to connect to the core server. Please see System Administration—Probes 881 (Probe Connection Settings) section for more information. *Note:* Also check the allowed and denied IPs there to make sure the core server accepts the IP address of the remote probe.

Probe Settings—Outgoing IP for monitoring requests

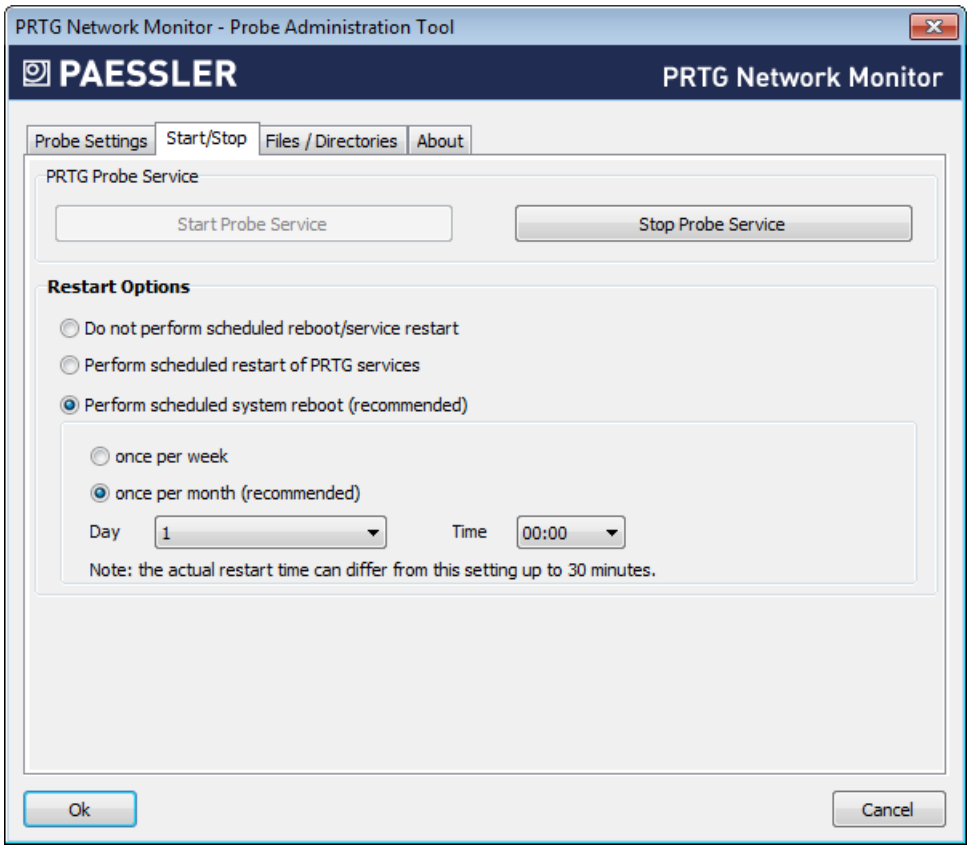
- If there is more than one IP on the current system available, you can specify the IP address that will be used for outgoing monitoring requests of certain sensor types.
- This setting will be used for sensors using the following connection types: HTTP, DNS, FTP, IMAP, POP3, Port, Remote Desktop, and SMTP.
- This is useful for devices that expect a certain IP address when queried.
- Default setting is **auto**. PRTG will select an IP address automatically.

Probe Settings—Probe Administration Tool Language

- Choose the language for this program from the drop down menu. Default is **English**. Depending on your installation, you may be able to choose other languages here.

Start/Stop

Start or stop the probe Windows service and schedule system restarts.



Start/Stop—PRTG Probe Service

You can stop and start the probe Windows service manually. Click the **Stop Probe Service** button to stop the service, and **Start Probe Service** to start it again. Both actions usually take from a few seconds up to several minutes to complete.

Start/Stop—Restart Options

For best performance we recommend to restart the Windows servers PRTG is running on from time to time. In order for PRTG to do this automatically you can schedule an automatic reboot. There are the following options:

Do not perform scheduled reboot/service restart

- Do not perform any scheduled reboot or restart of services automatically.
- We recommend a manual restart every few weeks.

Perform scheduled restart of PRTG services

- Restart both core server and probe service.
- Please enter a schedule below.

© 2011 Paessler AG

Perform scheduled system reboot (recommended)

- This is the recommended setting, although not set by default.
- Please enter a schedule below.
- We recommend restarting Windows servers once a month for best performance.

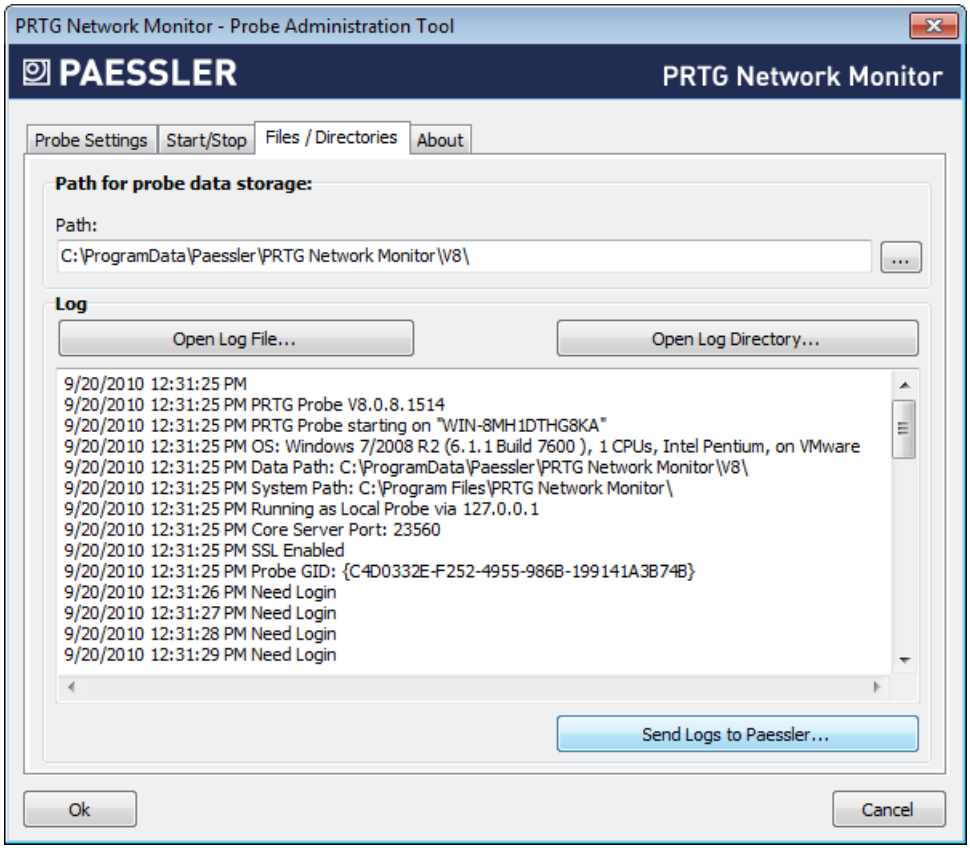
[Schedule]

When scheduling an automatic service restart or reboot, define a schedule. The options are:

- **Once per Week**: Select a weekday and time below.
- **Once per Month**: Select a day of month and time below. When selecting **Last**, the report will always run on the last day of the month, regardless of how many days the month has. When selecting a date that does not exist in every month, e.g. the 30th in May, PRTG will automatically run the report on the last day of this month.

Note: A Windows warning message will be displayed 10 minutes before reboot to inform a logged in user. The actual restart time can differ up to 30 minutes from the settings entered here!

Logs/Directory


PRTG Network Monitor - Probe Administration Tool
PAESSLER
PRTG Network Monitor
Probe Settings
Start/Stop
Files / Directories
About
Path for probe data storage:
Path:
C:\ProgramData\Paessler\PRTG Network Monitor\V8\
...
Log
Open Log File...
Open Log Directory...
9/20/2010 12:31:25 PM
9/20/2010 12:31:25 PM PRTG Probe V8.0.8.1514
9/20/2010 12:31:25 PM PRTG Probe starting on "WIN-8MH1DTHG8KA"
9/20/2010 12:31:25 PM OS: Windows 7/2008 R2 (6.1.1 Build 7600), 1 CPUs, Intel Pentium, on VMware
9/20/2010 12:31:25 PM Data Path: C:\ProgramData\Paessler\PRTG Network Monitor\V8\
9/20/2010 12:31:25 PM System Path: C:\Program Files\PRTG Network Monitor\
9/20/2010 12:31:25 PM Running as Local Probe via 127.0.0.1
9/20/2010 12:31:25 PM Core Server Port: 23560
9/20/2010 12:31:25 PM SSL Enabled
9/20/2010 12:31:25 PM Probe GID: {C4D0332E-F252-4955-986B-199141A3B74B}
9/20/2010 12:31:26 PM Need Login
9/20/2010 12:31:27 PM Need Login
9/20/2010 12:31:28 PM Need Login
9/20/2010 12:31:29 PM Need Login
Send Logs to Paessler...
Ok
Cancel

Path for probe data storage

- *Note:* This setting is relevant merely for probe only installations, for example, when running a remote probe on the system. For an installation of PRTG core server and probe, i.e. a full PRTG installation, the path setting in this window is overridden by the path defined in the settings of PRTG Server Administrator 957.

- Define the data folder to which PRTG will store configuration and monitoring data. *Note:* Before changing the path, make sure you stop both services and copy all data to the new location.

Log

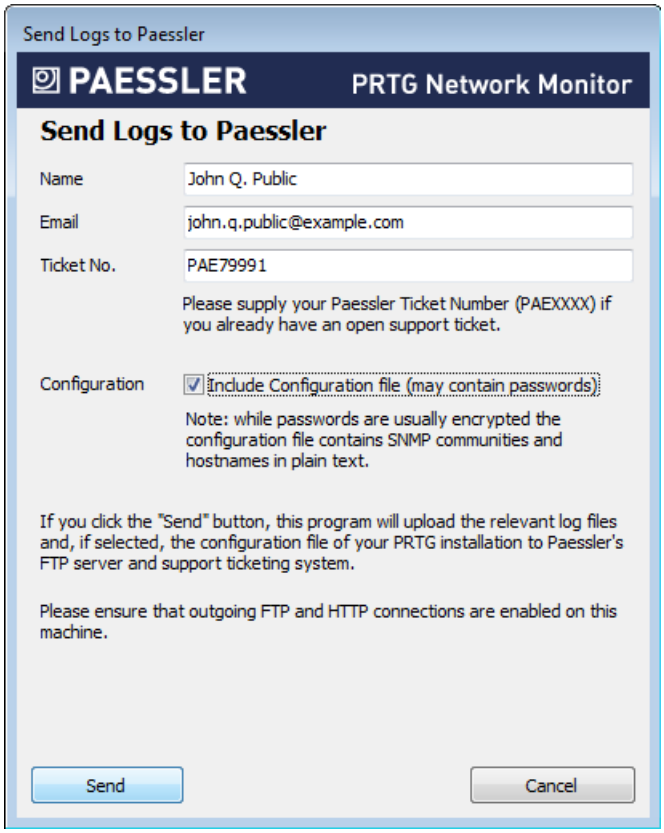
You can view the log of your PRTG probe. The following buttons are available:

- **Open Log File...**
  Directly view the content of the probe system log. Depending on the number of entries, it may take a few seconds until the logs are shown.

- **Open Log Directory...**
  Open the log file directory on your hard disk drive.

- **Send Logs to Paessler...**
  Open an assistant to send log files to the Paessler support team. Please see below.

Logs/Directory—Send Logs to Paessler


Send Logs to Paessler
PAESSLER
PRTG Network Monitor
Send Logs to Paessler
Name
John Q. Public
Email
john.q.public@example.com
Ticket No.
PAE79991
Please supply your Paessler Ticket Number (PAEXXXX) if you already have an open support ticket.
Configuration
Include Configuration file (may contain passwords)
Note: while passwords are usually encrypted the configuration file contains SNMP communities and hostnames in plain text.
If you click the "Send" button, this program will upload the relevant log files and, if selected, the configuration file of your PRTG installation to Paessler's FTP server and support ticketing system.
Please ensure that outgoing FTP and HTTP connections are enabled on this machine.
Send
Cancel

© 2011 Paessler AG

When opening a support ticket, Paessler support may ask you to send log files for further analysis. Using the **Send Logs to Paessler...** button, PRTG will automatically collect, compress and send your log files.

Name

- Please enter your name.

Email

- Please enter your valid email address.

Ticket No.

- This field is optional.
- If you have already opened a ticket at Paessler support, please provide the ticket number you received. Your files will then be associated with your ticket automatically.
- Please enter the ticket number starting with **PAE** followed by four or more digits.
- If you do not have a ticket number, please leave the field empty. *Note:* You should usually contact the support team *before* sending any files.

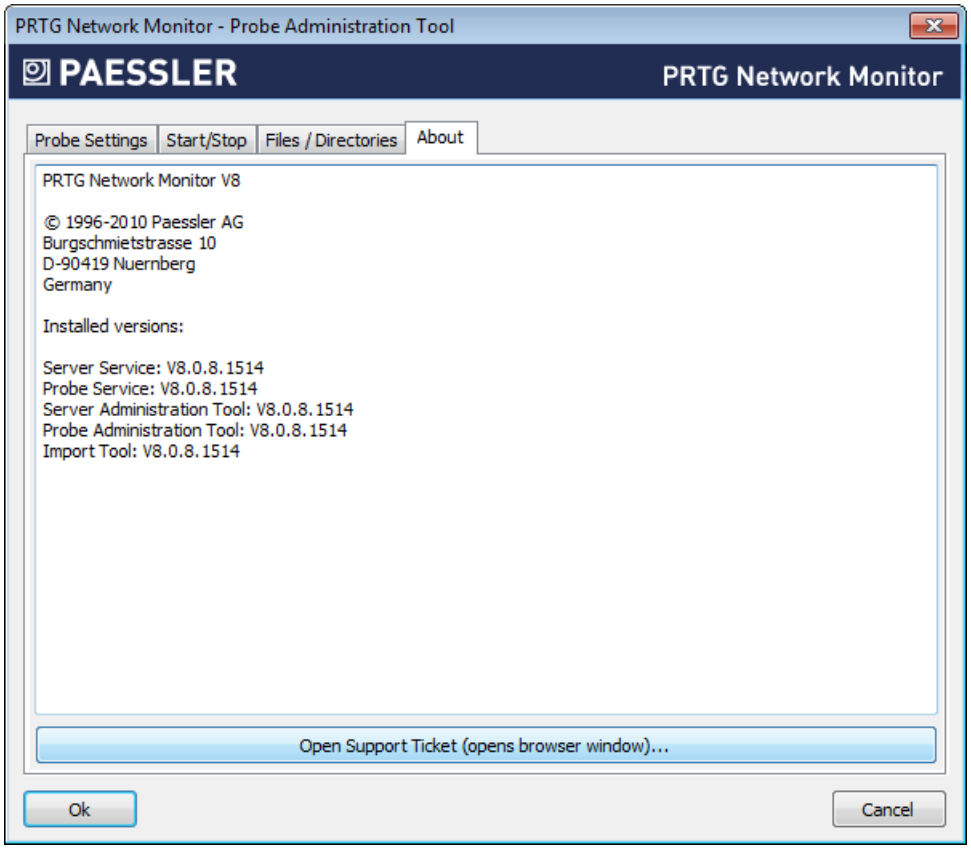
Configuration

- Define if your configuration file will be included in the data. Passwords are usually encrypted, but there may be some passwords stored as plain text.

Click on the **Send** button to start data upload. Please make sure FTP and HTTP connections are allowed on this machine.

© 2011 Paessler AG

About



Displays version information for installed PRTG programs. Click on the **Open Support Ticket** button to ask the Paessler support team for help. This will open a new web browser window.

© 2011 Paessler AG

Part XII

Advanced Topics

12 Advanced Topics

In this section topics are covered that address more advanced PRTG users. If you already gained some experience with PRTG, you might want to learn more about the topics following.

Advanced Topics—Topics

- Application Programming Interface (API) Definition 979
- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Channel Definitions for xFlow and Packet Sniffer Sensors 982
- Define IP Ranges 984
- Add Remote Probe 986
- Calculating Percentiles 995

© 2011 Paessler AG

12.1 Application Programming Interface (API) Definition

The PRTG Application Programming Interface (API) enables you to access monitoring data and manipulate objects using HTTP requests, run your own written sensors and notifications, and customize the web interface.

Detailed HTTP API Documentation

An interactive documentation of the API is integrated into your PRTG installation: Login to the web interface 94 and select **Setup | PRTG API** from the main menu.

In different tabs, the documentation provides information about:

- **HTTP API**: Access monitoring data and manipulate monitoring objects using HTTP requests (includes an interactive query builder)
- **Custom Sensors**: Create your own sensors for customized monitoring
- **Custom Notifications**: Create your own notifications to send alarms to external systems
- **Website Styling**: Customize the look and feel by adding your own CSS statements

You can also have a look at Paessler's PRTG demo installation's API documentation. But only the documentation that comes with your PRTG installation fits exactly the PRTG version you are using.

More

API Documentation in Paessler's PRTG Demo Installation

- http://prtg.paessler.com/api.htm?username=demo&password=demodemo

12.2 Filter Rules for xFlow and Packet Sniffer Sensors

Filter rules are used for the include, exclude and channel definition fields of Custom Packet Sniffer and Custom xFlow sensors. They are based on the following format:

```
field[filter]
```

Valid Fields for All Sensors

- **IP**
- **Port**
- **SourceIP**
- **SourcePort**
- **DestinationIP**
- **DestinationPort**
- **Protocol**
  Possible Protocol values: *TCP*, *UDP*, *ICMP*, *OSPFIGP*, or any number)
- **ToS**

Additional Fields for Packet Sniffer Sensors Only

- **MAC**
- **SourceMAC**
- **DestinationMAC**
- **EtherType**
  Possible EtherType values: *IPV4*, *ARP*, *RARP*, *APPLE*, *AARP*,*IPV6*,*IPXold*, *IPX*, or any number

Additional Fields for NetFlow v5 and jFlow v5 Sensors Only

- **Interface**
- **ASI**
- **InboundInterface**
- **OutboundInterface**
- **SourceASI**
- **DestinationASI**

Additional Fields for xFlow v9 Sensors Only

- **Interface**
- **ASI**
- **InboundInterface**
- **OutboundInterface**
- **SourceASI**
- **DestinationASI**
- **MAC**
- **SourceMAC**
- **DestinationMAC**
- **Mask**
- **DestinationMask**
  Note: "Mask" values represent subnet masks in the form of a single number (number of contiguous bits).

© 2011 Paessler AG

- **NextHop (IP address)**
- **VLAN**
- **SourceVLAN**
- **DestinationVLAN**
  Note: "VLAN" valuesrepresent a VLAN identifier.

Additional Fields for sFlow Sensors Only

- **Interface**
- **InboundInterface**
- **OutboundInterface**
- **MAC**
- **SourceMAC**
- **DestinationMAC**

Valid Data Formats

- IP fields support wildcards (*), range (10-20) and hostmask (/10, /255.255.0.0) syntax.
- Number fields support range (80-88) syntax.
- Protocol and EtherType fields support numbers and a list of predefined constants.

For detailed information on IP ranges, please see Define IP Ranges 984 section.

Examples

All of the following filter rules are valid examples:

```
SourceIP[10.0.0.1]
SourceIP[10.*.*.*]
SourceIP[10.0.0.0/10]
DestinationIP[10.0.0.120-130]
DestinationPort[80-88]
Protocol[UDP]
```

Complex expressions can be created using parentheses **( )** and the words **and**, **or**, or **not**. For example, this is a valid filter rule:

```
Protocol[TCP] and not (DestinationIP[10.0.0.1] or SourceIP[10.0.0.120-130])
```

Related Topics

- Channel Definitions for xFlow and Packet Sniffer Sensors 982
- Monitoring Bandwidth via Packet Sniffing 940
- Monitoring Bandwidth via Flows 942

12.3 Channel Definitions for xFlow and Packet Sniffer Sensors

When adding Custom xFlow sensors or Custom Packet Sniffing sensors, you will notice a field entitled **Channel Definition**. In this field you need to provide the channel definitions in the following syntax (one entry per channel):

```
#<id>:<Name>
<Rule>
```

Syntax

- **<id>** needs to be 1 or greater and must be unique for the sensor (i.e. each channel definition must have a unique id).
- The **<id>** is linked to the historic data: As soon as it has been changed, the history for this particular channel is lost.
- One rule can span multiple lines.
- The next rule starts with a # as first character in a line.
- **<name>** is the channel's display name.
- The rules are processed top to bottom (the number doesn't matter) and the data is accounted to the first match.
- One **Other** channel is added automatically.
- Behind the name a optional **[<unit>]** can be used to override the automatic unit based on the source sensors.

The **<Rule>** syntax is identical to the one described in the Filter Rules for xFlow and Packet Sniffer Sensors 980 section. Since data is accounted to the first match, please make sure to start with the most specific rule at the top getting less specific to the bottom.

Note: We recommend writing the rule list in an external editor and paste it into the respective PRTG field. Otherwise, if the rules contain an error, the entries will be removed when adding the rules in case!

Example

General example:

```
#5:HTTP
Protocol[TCP] and
(SourcePort[80] or DestinationPort[80] or SourcePort[8080] or
DestinationPort[8080])
```

Channel definition example for differentiating by protocol:

```
#1:TCP
Protocol[TCP]

#2:UDP
Protocol[UDP]

#3:ICMP
Protocol[ICMP]
```


© 2011 Paessler AG

Related Topics

- Filter Rules for xFlow and Packet Sniffer Sensors 980
- Monitoring Bandwidth via Packet Sniffing 940
- Monitoring Bandwidth via Flows 942

More

Knowledge Base: Can I add custom channels to standard Packet Sniffer and NetFlow sensors?

- http://www.paessler.com/knowledgebase/en/topic/2143

12.4 Define IP Ranges

In some setting fields, you can either enter a host name or single IP address, or you can define IP ranges. PRTG follows a common syntax for this. IP ranges are available, for example, for xFlow and Packet Sniffer sensors 203, and for probes settings 881.

Note: For the syntax available for PRTG's automatic network discovery, please see **Auto-Discovery** 147 (*IP Selection Method* setting).

Available Options

Option	Description	Syntax	Example(s)
Simple	Enter a fixed IP address.	a.b.c.d	10.0.10.9
Hostname	Enter a hostname. PRTG will resolve it to an IP address in your network.	hostname	device-xyz
Hostmask	Enter a hostmask. A hostmask defines the relevant bits of the IP address.	**a.b.c.d/h** *or* **a.b.c.d/e.f.g.h**	10.0.0.0/255
Range	Enter an IP address range. Please replace each of **a**, **b**, **c**, **d** by either ▪ * (asterisk) for any value; corresponds to *0-255* —or— ▪ **x-y** for any range between *0* and *255*.	**a.b.c.d**	10.0.0.1-20 *or* 10.*.0.* *or* 10.0.0-50.*

© 2011 Paessler AG

12.5 Regular Expressions

For some sensors, you can use regular expressions to match a search pattern. PRTG will use standard regexp. In the following, we will provide examples for the most common patterns.

Common Search Patterns

Find matches containing the word **error** *or* **alarm**:

```
\b(error|alarm)\b
```

Find matches containing the words **error** *and* **alarm** in any order:

```
(?=.*\berror\b)(?=.*\balarm\b).*
```

Find matches containing all of the words **tree**, **flower**, **leaf**, *and* **bug**, in any order:

```
(?=.*\btree\b)(?=.*\bflower\b)(?=.*\bleaf\b)(?=.*\bbug\b).*
```

Example

The search pattern

```
(?=.*\berror\b)(?=.*\balarm\b).*
```

would match the following lines:

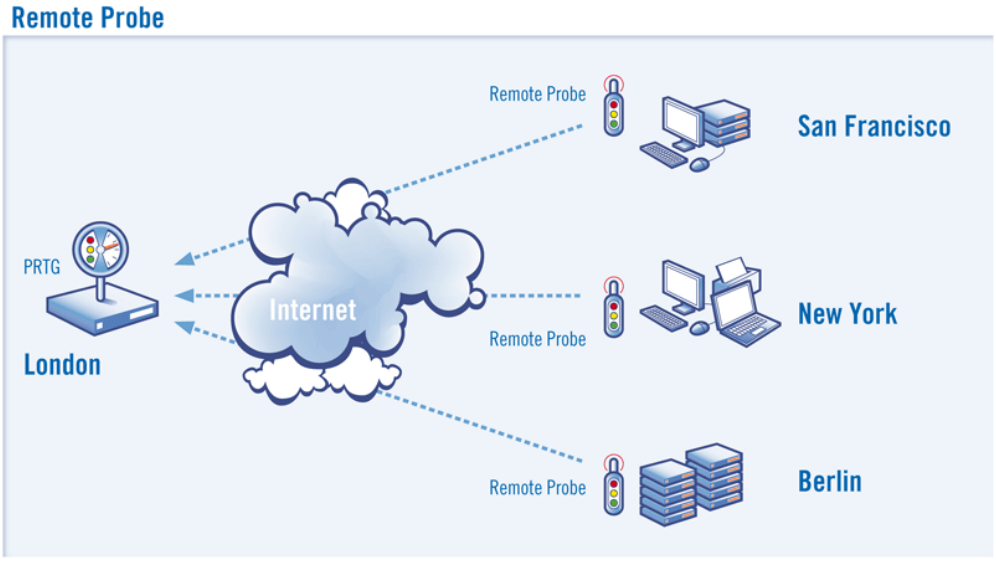
- alarm error
- error alarm
- I am an error and I evoke an alarm
- I am an alarm and indicate an error
- An alarm combined with an error indeed!
- An error combined with an alarm, too!

More

Regex Tester: Test Regular expressions interactively
- http://www.regexpal.com

Wikipedia: Regular expression
- http://en.wikipedia.org/wiki/Regular_expression

12.6 Add Remote Probe



Monitoring Remote Locations via Remote Probes

To monitor different sub-networks that are separated by a firewall, to keep an eye on remote locations, or for several other scenarios, you can extend your monitoring by installing one or more so-called **Remote Probes**.

Extend your Monitoring Now

Installing remote probes is easy and done in a few minutes. Please see the sections linked below for further instructions.

- Background: Remote Probes and Multiple Probes 987
- Step by Step: Remote Probe Setup 990

More

Video Tutorial: Core Server and Remote Probes

- http://www.paessler.com/support/video_tutorials/distributed_monitoring

© 2011 Paessler AG

12.6.1 Remote Probes and Multiple Probes

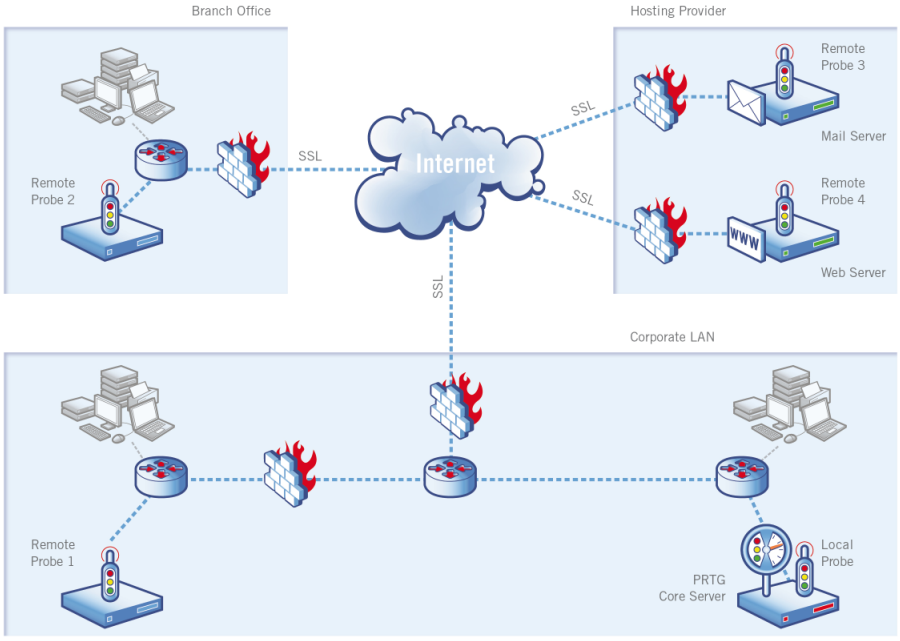
Upon installation, PRTG creates the first probe automatically, called the **Local Probe**. It runs on the same machine as the PRTG core server and monitors all devices from this system, using the sensors you have configured. Working with only one local probe should suffice for Local Area Network (LAN) monitoring and if you want to monitor one location only.

Scenarios Requiring Remote Probes

However, there are several situations that make it necessary to work with so-called **Remote Probe** in the same LAN or in remote locations. Among these are:

- You have more than one location and you need to make sure that services are available from all locations.
- Your network is separated in several LANs by firewalls and the local probe can not monitor specific services across the firewalls.
- You need to monitor systems in a Virtual Private Network (VPN) across public or in-secure data lines.
- You want to sniff packets on another computer.
- You want to monitor NetFlow data on another computer.
- You experience performance issues with CPU intensive sensors like packet sniffer or NetFlow sensors and need to distribute the load over more than one PC.

The following chart shows an example.



Monitoring a Distrubuted Network with PRTG (Illustration Also Available as Video Tutorial)

The PRTG core server inside the *Corporate LAN* (bottom right) is able to monitor:

- Services inside the *Corporate LAN* using the **Local Probe**.
- Services behind a firewall in the *Corporate LAN* using **Remote Probe 1**.

- Secured services inside the *Branch Office* (top left) using **Remote Probe 2**.
- Secured services on *Mail Server* and *Web Server* using **Remote Probe 3** and **Remote Probe 4** installed directly on these servers.
- Public services on the Internet using any of the probes.

How Probes Work

As soon as a probe is started it automatically connects to its core server 75, downloads the sensor configuration and begins its monitoring tasks. The core server sends new configuration data to a probe as soon as the monitoring configuration is changed by the user. Probes monitor autonomously and send the monitoring results back to the core server for each check they have performed. If the connections between core and probe fails for any reason (for example, a reboot of the computer running the core server) the probe continues its monitoring and stores the results. During a connection loss a buffer stores a maximum of 500,000 sensor results in RAM memory of the remote probe system (up to 50 - 200 MB). This means that for 100 sensors with one minute interval the monitoring results of up to 3 days can be buffered (or 52 minutes for 10,000 sensors with one minute interval). The probe automatically reconnects to the core as soon as it is available again and transmits all monitoring results gathered during the connection loss.

The connection between probe and core is initiated by the probe, secured using Secure Sockets Layer (SSL). This means that the data sent back and forth between core and probe is not visible to someone capturing data packets. The core server provides an open TCP/IP port and waits for connection attempts from probes. If a new probe connects for the first time the administrator will receive a ToDo and will then see the new probe in the sensor tree. As a security precaution, the probe must be manually acknowledged by the administrator in the **ToDos** list before any sensors can be created and monitored. The administrator can also deny a probe which will then be disconnected. No further connection attempts will be accepted and the probe IP is added to the **Deny IPs** list in the probes system settings (see **System Administration—Probes** 881 section). This ensures that unauthorized probes can not connect to a core server.

Since the probe initiates the connection, you must ensure that a connection can be established from the outside world onto your core server, e.g. you may need to open any necessary ports in your firewall and you may need to specify a Network Address Translation (NAT) rule for your network. The process is the same as if you want to allow access to the web server provided by the PRTG core server via port 443, for example.

Automatic Probe Update

Whenever a new version of PRTG is installed on the core server all remote probes will automatically download and install the updated version of the probe as soon as they reconnect to the updated core installation.

The local probe has already been updated during the core installation. All remote probes are automatically downloading the new binaries using the SSL-secured probe/core connection. The download of the 4 MB file takes between a few seconds (in a LAN) and a few minutes (via Internet connections), depending on the available bandwidth. As soon as the update has been downloaded the probe disconnects, installs the update and reconnects to the core server. This takes between 20 and 100 seconds. Please note that during the update phase the monitoring of the local probe can be affected due to the bandwidth required for the downloads.

© 2011 Paessler AG

More

- Remote Probe Setup 990

Video Tutorial: There is a video available on the Paessler video tutorials page.
- http://www.paessler.com/support/video_tutorials

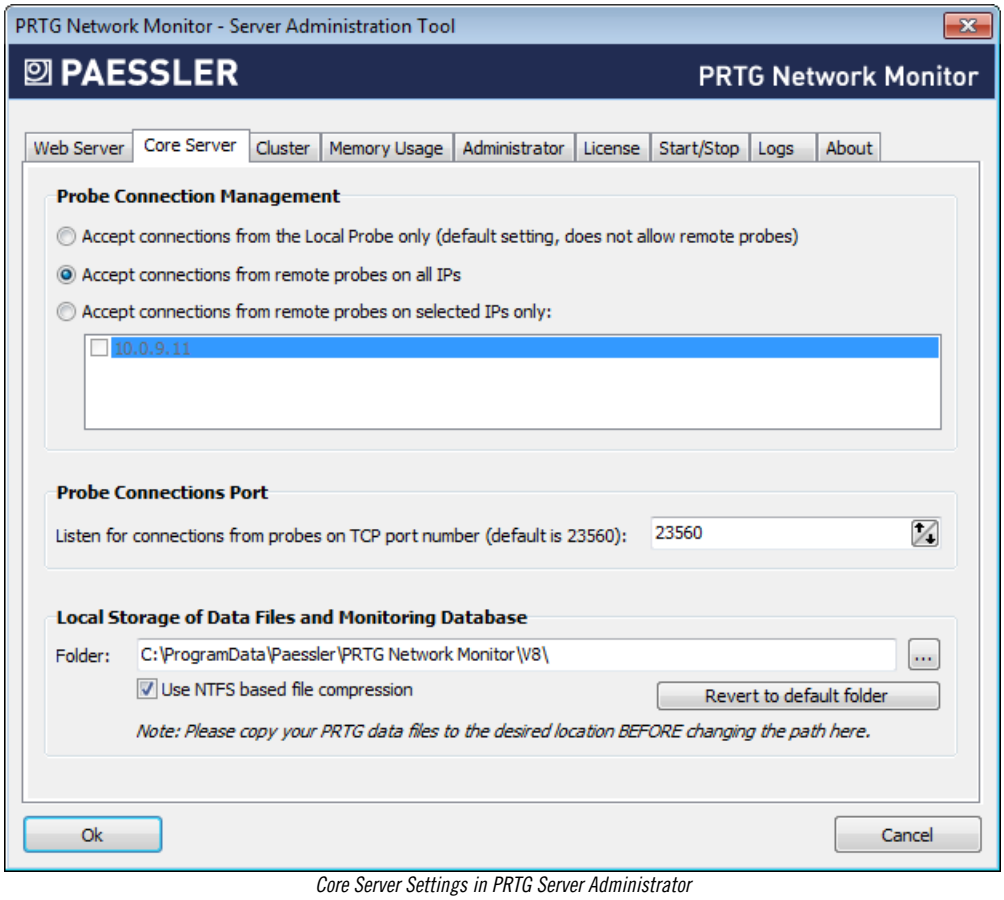
12.6.2 Remote Probe Setup

This section will guide you through some easy steps to set up a remote probe.

- Step 1: Prepare Core Server 990
- Step 2: Settings in Web Interface 991
- Step 3: Download and Install Remote Probe 992
- Step 4: Configure Remote Probe Connection 992
- Step 5: Approve New Probe and Start Monitoring 993
- Debugging Probe Connection Problems 994

Step 1: Prepare Core Server

Before remote probes can connect to the core server you must edit the relevant settings in the **PRTG Server Administrator** 957.


PRTG Network Monitor - Server Administration Tool
PAESSLER
PRTG Network Monitor
Web Server
Core Server
Cluster
Memory Usage
Administrator
License
Start/Stop
Logs
About
Probe Connection Management
Accept connections from the Local Probe only (default setting, does not allow remote probes)
Accept connections from remote probes on all IPs
Accept connections from remote probes on selected IPs only:
10.0.9.11
Probe Connections Port
Listen for connections from probes on TCP port number (default is 23560):
23560
Local Storage of Data Files and Monitoring Database
Folder:
C:\ProgramData\Paessler\PRTG Network Monitor\V8\
Use NTFS based file compression
Revert to default folder
Note: Please copy your PRTG data files to the desired location BEFORE changing the path here.
Ok
Cancel

Core Server Settings in PRTG Server Administrator

By default, a core server accepts connections **from the Local Probe only**. This setting does not allow remote probes, which is the most secure setting. In order to allow external probes to connect, please change to the **Core Server** tab, and in the **Probe Connection Management** section, choose one of the following options:

© 2011 Paessler AG

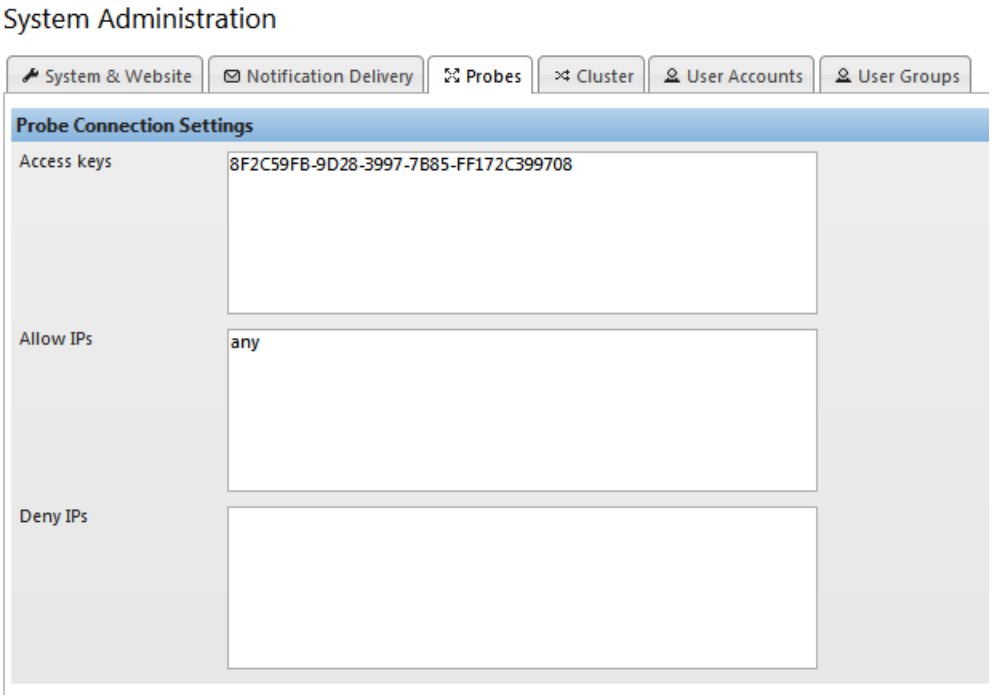
- **Accept connections from remote probes on all IPs**: We recommend using this setting for easy setup.
- **Accept connections from remote probes on selected IPs only**: Specify the IP addresses that will accept incoming connections.
- As **Probe Connections Port**, you can leave the standard port number, even when configuring several probes. Please make sure this port is not blocked by firewall rules on your core server's side. You have to configure the same port number in your remote probe's settings, so please save it for later use.

When you are done, click **OK** to save your settings. The core server process must be restarted so that the changes take effect.

For detailed information about these settings, please see PRTG Server Administrator 957 (**Core Server**) section.

Step 2: Settings in Web Interface

Login to the Ajax web interface 94. From the main menu, select **Setup | System Administration | Probes** to access the probes settings.



Probes Settings in System Administration

- From the **Access keys** field, copy one access key you will use for the remote probe connection. You can also enter a new access key if you like. In any case save the correct access key for later use.

- In the **Allow IPs** field, enter the IP address of the computer you will install a remote probe on. To make things easier, you can also enter the word **any**; this will set the core server to accept remote probes connecting from any IP address.

- Make sure the IP address of the computer you will install a remote probe on is not listed in the **Deny IPs** field.

For detailed information about these settings, please see **System Administration—Probes** 881 section.

Step 3: Download and Install Remote Probe

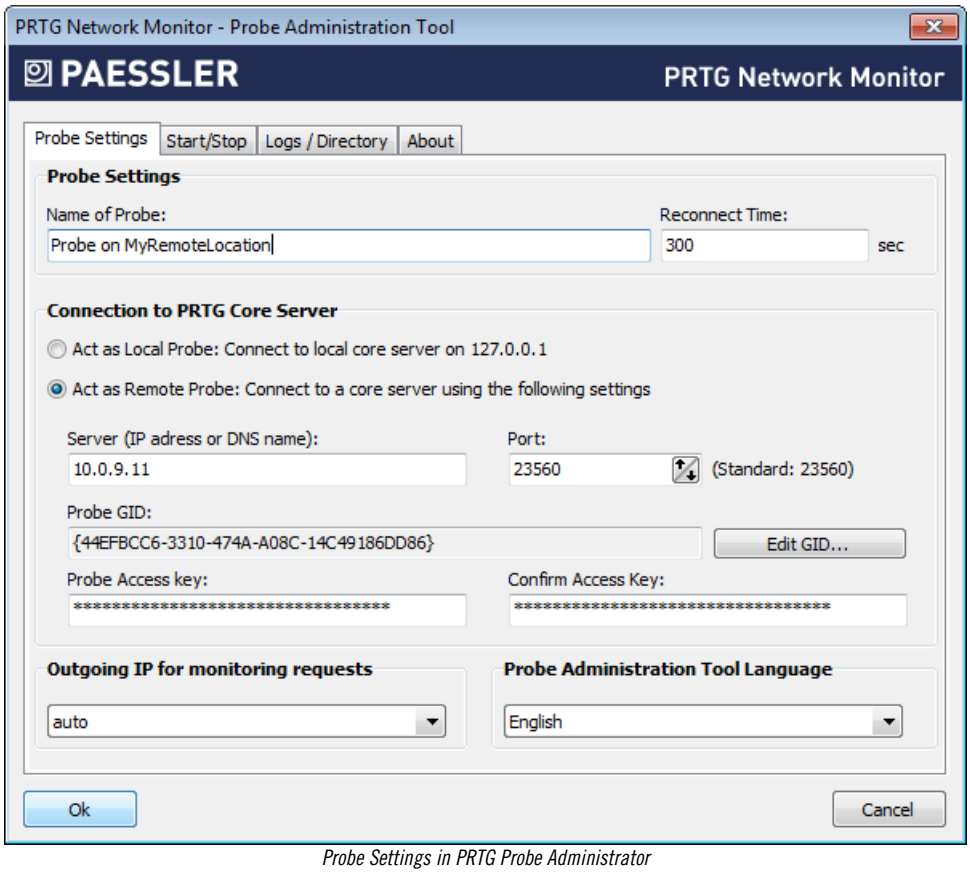
From the computer you want to install a remote probe on, connect to the Ajax web interface 94, download the setup file and install it. For detailed instructions, please see **Install a PRTG Remote Probe** 59 section. *Note:* You cannot install a remote probe on a system already running a PRTG core installation.

At the end of the remote probe installation the **PRTG Probe Administrator** will be started (or you can start it manually from the Windows start menu later).

Step 4: Configure Remote Probe Connection

In the **PRTG Probe Administrator** 969 on the Windows system you have installed the remote probe on, please configure the connection to the core server.

© 2011 Paessler AG



Probe Settings in PRTG Probe Administrator

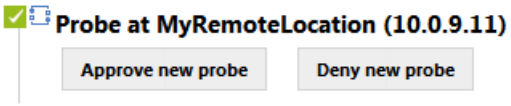
In the **Connection to PRTG Core Server** section, select the **Act as Remote Probe** option. You can then edit the following settings:

- **Server**: Enter the IP address of DNS name of the core server the remote probe will connect to. If Network Address Translation (NAT) is used, this must be the IP address that is externally visible, as the remote probe will connect from outside of your network.
- **Port**: Enter the port number the remote probe will connect to on the core server. This number must match the one set in Step 1 990.
- **Probe Access Key** and **Confirm Access Key**: Enter the access key the probe will send to the core server. You have saved this key in Step 2 991. This key has to match exactly the one shown in the web interface's probes settings, so a connection can be established.

For detailed information about these settings, please see **PRTG Probe Administrator** 969 section. Click the **Ok** button to confirm your settings and to start the probe service.

Step 5: Approve New Probe and Start Monitoring

When a new probe connects to the core server for the first time, a new ToDo 117 will be created and it will show up as a new object in the device tree of your setup.



Approve New Probe

Please click on **Approve New Probe** to fully enable the probe. You have to do this once for every new probe. Once approved, PRTG automatically creates a set of sensors for the probe to ensure that bottle-necks on the probe will always be noticed. We recommend keeping these sensors. You can now create groups, devices and sensors for monitoring via the new probe.

Debugging Probe Connection Problems

If you have trouble with the setup of remote probes please look at the probe's log files.

The probe process writes log files with a file name in the format **PRTG Probe Log (*x*).log**. Please open the one with the most recent date.

For a correct connection the probe log should look similar to this:

```
11.11.2010 16:15:15 PRTG Probe Server V8.1.2.5101
11.11.2010 16:15:15 Starting Probe on "WINXPVMWARE"
11.11.2010 16:15:15 Data Path: C:\documents and settings\All Users\a[...]
11.11.2010 16:15:15 Local IP: 0.0.0.0
11.11.2010 16:15:15 Core Server IP and Port: 10.0.2.167:23560
11.11.2010 16:15:15 Probe ID: -1
11.11.2010 16:17:01 Connected to 10.0.2.167:23560
11.11.2010 16:17:06 Login OK: Welcome to PRTG
```

If the connection fails, for example, due to an incorrect **Access Key**, you will see:

```
11.11.2010 16:31:02 Try to connect...
11.11.2010 16:31:02 Connected to 10.0.2.167:23560
11.11.2010 16:31:07 Login NOT OK: Access key not correct!
```


© 2011 Paessler AG

12.7 Calculating Percentiles

Wikipedia describes a percentile as *the value of a variable below which a certain percent of observations fall*. Providers often use it in their billing models, e.g. when determining the used bandwidth. With percentile calculation, you can cut off an x percent of peak values from a certain amount of values.

In PRTG, you can calculate percentiles when creating general reports (see **Reports** 827 section) or creating historic data reports of a certain sensor (see **Historic Data Reports** 107 section). If you activate the **Percentile Results** option in your reports' settings, the according values will be added to the tables. You can customize the following settings:

- **Percentile**: Enter the percentile number you want to calculate. If you choose, for example, to calculate the 95th percentile, enter "95" here and 5 % of peak values will be discarded.
- **Percentile Average**: This is the averaging interval in seconds, which is used for percentile calculation. Default value is 300 which is equivalent to 5 minutes.

Percentile Mode: Choose between **Discrete** and **Continuous**. Continuous percentile interpolates between discrete values, whereas discrete percentile chooses the next smaller discrete value.

- **Discrete** percentile means that the value must be a member of the data set. For this kind of calculation you require a discrete distribution. The median of a discrete distribution can not be defined, as such, meaning that the 50th discrete percentile may not necessarily be the median if the value does not belong to an odd number of measurements. Discrete percentiles, as such, should not be used for billing applications.
- **Continuous** percentile basically means that the measurements are treated as a statistical population and the value is determined by interpolating a value when it isn't present. This means that values are interpolated between actual measurements that are varying around the "perfect" center of the measurements.

More

Knowledge Base: What are percentiles?

- http://www.paessler.com/knowledgebase/en/topic/9563

Part XIII

Appendix

13 Appendix

Please find further information in the following sections.

- Glossary 999
- List of Abbreviations 1002
- Support and Troubleshooting 1004
- Legal Notices 1005

© 2011 Paessler AG

13.1 Glossary

This section explains special words used in the context of PRTG Network Monitor. *Note:* Here, only explanations are given. For information on where to find detailed instructions for a specific key word, please see the **Index** section.

Channel

The monitoring data of a sensor 1001 is shown in sensor channels. For example, for sensors that measure network traffic, there is one channel each for traffic *in* and traffic *out*. You can set various triggers for each channel, enabling you to set sensor status changes or notifications based on the monitoring data received.

Cluster

PRTG can be configured as a failover cluster for fail-safe monitoring. In a cluster, one or more core servers 999 work together in one configuration. Every node can monitor all devices in a network for gapless monitoring, additionally enabling you to compare monitoring results measured from different perspectives.

Cluster Node

Sometimes used as synonym for Node 1000.

Cluster Probe

When running PRTG in cluster mode, a cluster probe is automatically created. All objects 1000 created on the cluster probe, or below it in the device tree 1000, are monitored by all nodes in the cluster. Create or move objects 1000 there to monitor them fail-safely. If one node fails, the other nodes will continue to monitor them. You can add groups 1000 and devices 999 to the probe. On a PRTG installation, the cluster probe runs as part of this installation's local probe 1000. Remote probes 1001 cannot be connected to a cluster probe, but only to one local probe of one PRTG installation.

Core Server

The central unit of PRTG. It receives monitoring data from the probe(s) 1001 and handles reporting and notifications, provides the web server for the user interfaces, and many other things. In a cluster 999, one core server is installed on every node.

Device

A device in PRTG represents a physical device in the network. For an easily understandable tree structure, you usually create one PRTG device for each physical device you want to monitor (exceptions apply to some sensors that can only be created on the local probe 1000 device, and for sensor types that are not bound to a certain device, such as HTTP sensors, which are also usually created on the local probe). You can add one or more sensors 1001 on every device.

Device Tree

PRTG's configuration is represented in a hierarchical tree structure, called device tree, containing all objects 1000. While building the tree, you can relate to your network's topology to make your monitoring setup easy to understand.

Failover Master (Node)

If the primary master 1001 node fails, a failover node 1000 is promoted to current failover master and takes over the master role until the primary master node re-joins the cluster 999.

Failover Node

In a cluster 999 a failover node monitors all sensors 1001 on the cluster probe 999, providing monitoring data for the core server 999. Additionally, it serves as a backup in case the master node 1000 fails.

Group

A group is an organizational unit in your PRTG tree structure that helps to arrange your devices. To existing groups, you can add devices, or additional sub-groups. This way you can model your physical network's topology within the PRTG configuration.

Local Probe

The local probe is installed together with the core server 999. All objects 1000 created on the local probe, or below it in the device tree 1000, are monitored by the local core system. You can add groups 1000 and devices 999 to the probe.

Master Node

In a cluster 999, the master node controls the settings and cluster management. It also takes over notifications. All changes to the monitoring configuration are made on the master node.

Node

In a cluster 999 there is one master node 1000 and one or more failover nodes 1000. On each node, one PRTG core server 999 installation is running independently. All nodes are connected to each other, exchanging configuration and monitoring data.

Object

All different items in the device tree 1000 are generally referred to as objects. An object can be a probe 1001, a group 1000, a device 999, or a sensor 1001.

© 2011 Paessler AG

Primary Master (Node)

The *primary* master node in a cluster 999 is the node 1000 that is master by configuration. Only if it fails, one of the failover nodes 1000 becomes failover master 1000 and takes over the master role until the primary master node re-joins the cluster.

Probe

On a probe, the actual monitoring takes place. A probe can run as local probe 1000 on the local system where the core server 999 is installed. There are also cluster probes 999 and remote probes 1001.

Remote Probe

A remote probe is a small piece of software installed on a computer in the local or remote network. It scans the network from there and sends monitoring results to the core server 999. Once the connection is established, the remote probe is shown in the PRTG tree structure. All objects 1000 created on the remote probe, or below it in the device tree 1000, are monitored by the remote system running the remote probe. You can add groups 1000 and devices 999 to the probe. In cluster 999, remote probes can only be connected to the master node 1000, not to one of the failover nodes 1000.

Sensor

A sensor monitors one aspect of a device 999. For example, monitoring if a device responds to a Ping request is done by one sensor. Monitoring the traffic of one ethernet port of a router device is done by another sensor. For monitoring the CPU load of the local system yet another sensor is set up, and so on. A sensor's data is shown in channels 999.

Sensor Tree

Sometimes used as synonym for device tree 1000.

ToDo

ToDos are created by the system and contain important messages or action steps to take for the administrator. Every ToDo should be acknowledged. You can access the list of ToDos from the main menu.

xFlow

Paessler designates all kinds of flow protocols as xFlow. Currently, PRTG supports NetFlow V5 and V9, sFlow V5, and jFlow V5.

© 2011 Paessler AG

13.2 List of Abbreviations

ADO: ActiveX Data Objects (ADO)

AJAX: Asynchronous Java Script and XML (AJAX)

API: Application Programming Interface (API)

CSV: Comma Seperated Values (CSV)

DHCP: Dynamic Host Configuration Protocol (DHCP)

DMZ: Demilitarized Zone (DMZ)

DNS: Domain Name Service (DNS)

GUI: Graphical User Interface (GUI)

GUID: Globally Unique Identifier (GUID)

HTTP: Hypertext Transfer Protocol (HTTP)

IMAP: Internet Message Access Protocol (IMAP)

LAN: Local Area Network (LAN)

LDAP: Lightweight Directory Access Protocol (LDAP)

MIB: Management Information Base (MIB)

MOS: Mean Opinion Score (MOS)

NAT: Network Address Translation (NAT)

NTP: Network Time Protocol (NTP)

PDF: Portable Document Format (PDF)

PDV: Packet Delay Variation (PDV)

POP3: Post Office Protocol version 3 (POP3)

RADIUS: Remote Authentication Dial-In User Service (RADIUS)

RPC: Remote Procedure Call (RPC)

© 2011 Paessler AG

SASL: Simple Authentication and Security Layer (SASL)

SLA: Service Level Agreement (SLA)

SMB: Server Message Block (SMB)

SMTP: Simple Mail Transfer Protocol (SMTP)

SNMP: Simple Network Management Protocol (SNMP)

SOAP: Simple Object Access Protocol

SPAN: Switched Port Analyzer (SPAN)

SQL: Structured Query Language (SQL)

SSH: Secure Shell (SSH)

SSL: Secure Sockets Layer (SSL)

TFTP: Trivial File Transfer Protocol (TFTP)

UNC: Uniform Naming Convention (UNC)

UUID: Universally Unique Identifier (UUID)

VoIP: Voice over IP (VoIP)

VPN: Virtual Private Network (VPN)

WAN: Wide Area Network (WAN)

WBEM: Web-Based Enterprise Management (WBEM)

WMI: Windows Management Instrumentation (WMI)

WQL: Windows Management Instrumentation Query Language (WQL)

XML: Extensible Markup Language (XML)

13.3 Support and Troubleshooting

Need help with PRTG? There are several ways to get support and trouble shooting.

Video Tutorials

A video says more than a thousand words—watch tutorials for PRTG from Paessler and other PRTG users.

- http://www.paessler.com/support/video_tutorials

Paessler Knowledge Base

In the Knowledge Base you can search in hundreds of articles about PRTG. You can post your own questions and answers, too!

- http://www.paessler.com/knowledgebase/

Open a Support Ticket

Users that have purchased a license can open support tickets which will usually be answered by Paessler's staff in less than 24 hours on business days.

- https://service.paessler.com/en/openticket/

© 2011 Paessler AG

13.4 Legal Notices

Build using Indy Internet Direct (http://www.indyproject.org/). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). Uses the net-SNMP library, see "netsnmp-license.txt". Uses the DelphiZip library distributed under the GNU LESSER GENERAL PUBLIC LICENSE (http://www.delphizip.net/). Uses the Info.Zip library, license info in the provided "info-zip-license.txt". Uses FastMM (http://sourceforge.net/projects/fastmm/) and TPLockBox (http://sourceforge.net/projects/tplockbox) under the Mozilla Public License 1.1 (MPL 1.1, available from http://www.mozilla.org/MPL/MPL-1.1.html). Soundfiles from http://www.soundsnap.com. Uses Public Domain regional maps from the "CIA World Factbook" webpage of the CIA (https://www.cia.gov/library/publications/the-world-factbook/docs/refmaps.html). Uses the "wkhtmltopdf" (http://code.google.com/p/wkhtmltopdf/) library distributed under the GNU LESSER GENERAL PUBLIC LICENSE (see wkhtmltopdf_lgpl-3.0.txt). Icons from http://www.androidicons.com.

All trademarks and names mentioned herein belong to their respective owners.

Index

- 2 -

2 days tab 104

- 3 -

30 days tab 104
365 days tab 104

- A -

Account Type 859
Add
  Device 160
  Group 157
  Sensor 165
Ajax Web Interface 92
Alarms 133
Android App
  PRTGdroid 930
API 979
Architecture
  Basic Concept 75
Audible Alarms 859
Auto-Discovery
  Quick Start 32
  Settings 145
Automatic
  Folding 859
  Refresh 859
  Restart Options (Probe System) 969
Averaging 107, 827

- B -

Bandwidth Monitoring Overview 944
Basic Concepts 74
Billing Tool 890

- C -

Change Trigger 797
Cluster
  Basic Concept 78
  Maintenance Mode 888
  Status 888
Cluster Connection 883
Configure
  Cluster 53, 883
  Dependencies 85
  Device 193
  Geographical Map 823
  Group 181
  Map 842
  Notification 825, 862
  Notification Delivery 877
  Notification Trigger 797
  Object Arrangement 811
  Probe 59, 173, 881, 969
  PRTG Server 45, 955
  Reboot (automatic) 969
  Report 827
  Root Group 166
  Schedule 868
  Sensor 202
  Sensor Channel 792
  System 857, 871
  User Account 859, 884
  User Group 887
  Website 871
Continuous (Percentiles) 995
Create Objects 156

- D -

Data Purging 871
Data Reporting 88
Date Format 859
Decimal Places 792
Dependencies 85
Device
  add 160
  arrange 811
  clone 817
  Template 815
Devices 133
Discrete (Percentiles) 995
Down 102
Down (Acknowledged) 102
Down (Partial) 102

© 2011 Paessler AG

Downloads
Add-Ons 890
Remote Probe Installer 890
Windows GUI Installer 890

- E -

Edit 124
Email Address 859
Email Round Trip
Technology 951
Email Templates 871
Error Limit 792

- F -

Flow
Channel Definitions 982
Filter Rules 980
IP Ranges 984
Technology 942
Toplists 807

- G -

Geo Map Type 871
Geographical Map 823
Google
Code 790
Maps 823
Graph
Settings 871
Type 871
Group
add 157
arrange 811
clone 817

- H -

Hash 859
Help Center 133
Home 133
Homepage 859
HTML GUI 927
HTTP Proxy 877

- I -

Inheritance of Settings 82
Intervals 871
iPhone App
iPRTG 930

- L -

L 97
Latency 797
Limits
Error 792
Warning 792
Line
Color 792
Width 792
Live Data tab 104
Login Name 859
Logout 133
Logs 133

- M -

M 97
Maintenance Mode 888
Maps 133, 842
audible alert 847
automatic rotation 842
Designer 847
edit 847
Line Color 847
Mini HTML 927
Move 124

- N -

Notification 825, 862
Delivery 877
Trigger 797
Notifying 87

- O -

Object Hierarchy 79

© 2011 Paessler AG

Off Notification 797
OK 102
On Notification 797
Overview tab 104

- P -

Packet Sniffer
  Channel Definitions 982
  IP Ranges 984
Packet Sniffing
  Filter Rules 980
  Technology 940
  Toplists 807
Passhash 859
Password 859
Pause 124
Paused 102
Peak Filter (Spike Filter) 792
Percentile 995
Percentiles 107, 827
Performance Strategy 871
Probe
  arrange 811
Probe Administrator 969
Probe Connection 881
Probes
  IP Ranges 984

- Q -

Quick Start Guide 26

- R -

Refresh 133, 859
Remote Probe 986
Remote Registry 656
Reports 133, 827
  Data 88
Restart Options (Probe System) 969

- S -

S 97
Scheduled Reboot (Probe System) 969
Scheduling 86
Search Box 133
Sensor
  add 165
  arrange 811
  Behavior 102
  Channel Settings 792
  clone 817
  compare 819
  Dependencies 821
  Multi-Edit 813
  Notification Trigger 797
  Settings 202
  Status 102
  Type 203
Sensors 133
Server Administrator 955
Session Expiry 871
Setup 133
Shift 847
SMS Delivery 877
SMTP Delivery 877
SNMP
  Technology 935
Sound Alarms 859
Speed Trigger 797
Spike Filter 792
State Trigger 797
System
  Status 888

- T -

Tags 84
Threshold Trigger 797
Timezone 859
ToDo Email Address 871
ToDos 133
Toplists 807
Tree view selection 97
Trigger
  Change 797
  Latency 797
  Speed 797
  State 797
  Threshold 797
  Volume 797

© 2011 Paessler AG

- U -

Undefined 102
Unusual 102
Unusual Detection 871
Uptime Threshold 871
User Access Rights 89
Username 859

- V -

Vertical Axis Scaling 792
VoIP
  Technology 947
Volume Trigger 797

- W -

Warning 102
Warning Limit 792
Web Interface 92
Web Server
  IP Address 871
  Port 871
Windows GUI 894
  Menu Structure 919
  Menu Tab 899
  Options 913
WMI
  Technology 938

- X -

XL 97

© 2011 Paessler AG

Last change to this manual (YYYY-MM-DD): 2011-05-17

© 2011 Paessler AG